



Q1. 解决方案架构师正在 Amazon API Gateway 背后设计一项新服务。服务的请求模式将是不可预测的，并且可能会突然从每秒 0 个请求更改为每秒超过 500 个。  
当前需要保留在后端数据库中的数据总大小小于 1 GB，并且未来的增长无法预测。可以使用简单的键值请求查询数据。哪种 AWS 服务组合可以满足这些要求？（选择两个）

- A.AWS Fargate
- B.AWS Lambda
- C.Amazon DynamoDB
- D.Amazon EC2 自动扩展
- E.与 MySQL 兼容的 Amazon Aurora

答案:BC

在这种情况下，AWS Lambda 可以执行计算并将数据存储在 Amazon DynamoDB 表中。Lambda 可以扩展并发执行以轻松满足需求，而 DynamoDB 是为满足键值数据存储需求而构建的，并且无服务器且易于扩展。因此，这是针对不可预测的工作负载的经济有效的解决方案。

正确：“AWS Lambda”是正确答案。

正确：“Amazon DynamoDB”也是正确的答案。

错误：“AWS Fargate”不正确，因为容器不断运行，因此即使没有请求，也会产生费用。

不正确：“Amazon EC2 Auto Scaling”不正确，因为它使用 EC2 实例，即使没有请求，这也会产生费用。

不正确：“Amazon RDS”不正确，因为这是关系数据库而不是 No-SQL 数据库。因此，它不适合键值数据存储要求。

参考文献:

<https://aws.amazon.com/lambda/features/>

<https://aws.amazon.com/dynamodb/>

Q2. 解决方案架构师需要为公司的应用程序设计一个托管的存储解决方案，其中包括高性能的机器学习。

该应用程序在 AWS Fargate 上运行，并且连接的存储需要并发访问文件并提供高性能。

解决方案架构师应建议哪种存储选项？

- A. 为应用程序创建一个 Amazon S3 存储桶，并为 Fargate 建立 IAM 角色以与 Amazon S3 通信。
- B. 创建一个用于 Lustre 文件共享的 Amazon FSx，并建立一个 IAM 角色，该角色允许 Fargate 与 FSx for Lustre 进行通信。
- C. 创建一个 Amazon Elastic File System (Amazon EFS) 文件共享，并建立一个 IAM 角色，该角色允许 Fargate 与 Amazon EFS 通信。
- D. 为应用程序创建一个 Amazon Elastic Block Store (Amazon EBS) 卷，并建立一个 IAM 角色，该角色允许 Fargate 与 Amazon EBS 通信。

答案:B

<https://aws.amazon.com/efs/>

关键字：并发访问文件+交付高性能 Amazon FSx-

为快速处理工作负载而优化的高性能文件系统. Lustre 是一种流行的开源并行文件系统.

还支持从数千个计算实例并发访问同一文件或目录.

带有 FSx 的 Amazon IAM-

Amazon FSx 与 AWS Identity and Access Management (IAM) 集成在一起。此集成意味着您可以控制您的 AWS IAM 用户和组可以采取的管理文件系统的操作（例如创建和删除文件系统）。您还可以标记您的 Amazon FSx 资源，并基于这些标记控制 IAM 用户和组可以执行的操作。

Fargate 启动类型-因此，根据尼尔·大卫·法尔盖特 (Neal David Fargate) 的回答，C & D 被排除在外

### Fargate 设置和管理计算

负责执行任务

没有 EFS 和 EBS 集成

Fargate 处理集群优化

控制有限，基础设施自动化

Q3. 一家公司拥有一个多层次的应用程序，该应用程序在应用程序负载平衡器 (ALB) 后面的单个可用区中的一个 Amazon EC2 Auto Scaling 组中运行六个前端 Web 服务器。解决方案架构师需要将基础结构修改为高度可用，而无需修改应用程序。

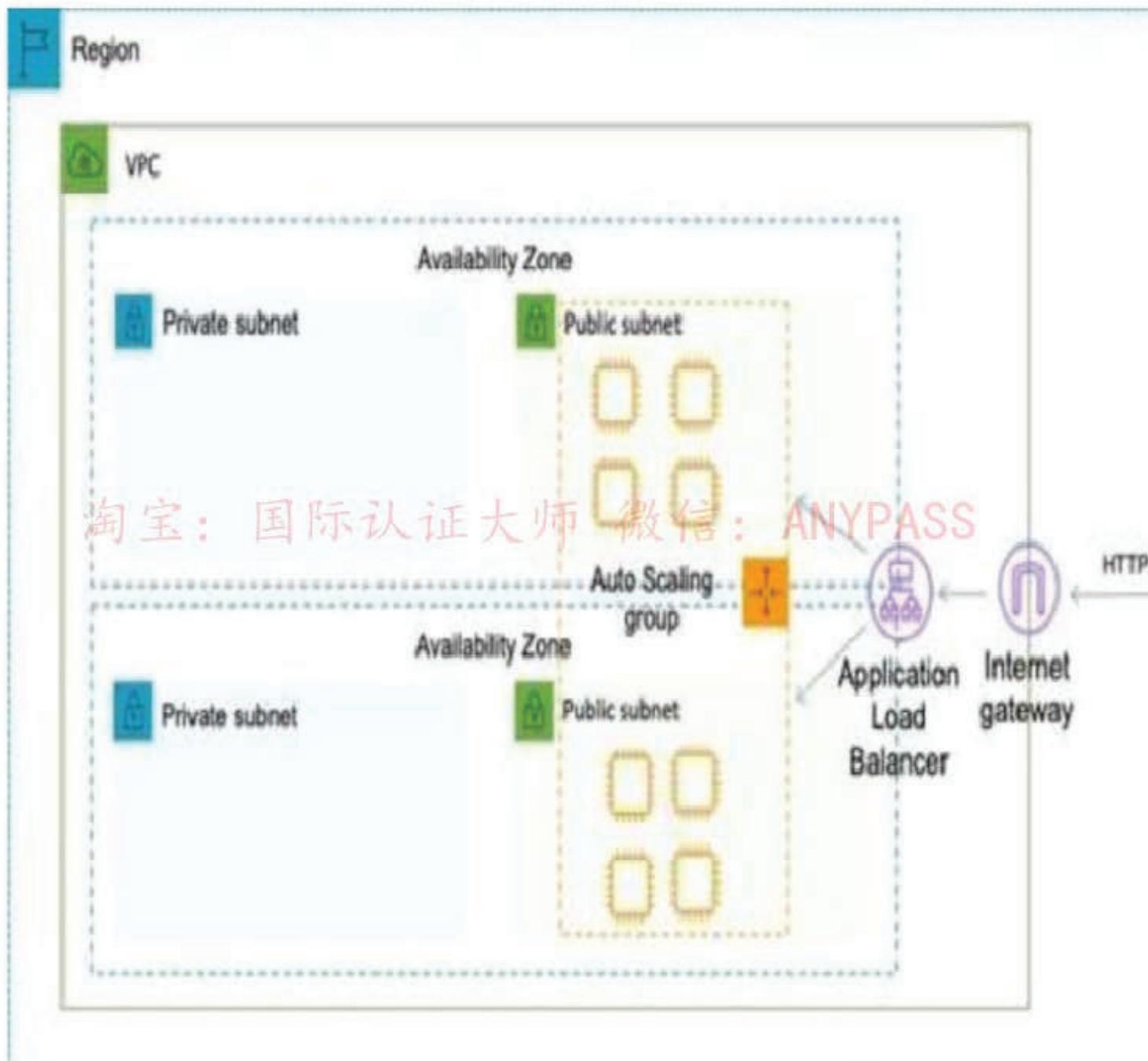
解决方案架构师应该选择哪种架构来提供高可用性？

- A. 创建一个 Auto Scaling 组，该组在两个区域的每个区域中使用三个实例
- B. 修改 Auto Scaling 组，以在两个可用区中的每个可用区中使用三个实例
- C. 创建一个 Auto Scaling 模板，该模板可用于在另一个 Region 中快速创建更多实例

D.在循环配置中更改 Amazon EC2 实例前面的 ALB，以平衡到 Web 层的流量

答案:B

通过修改现有的 Auto Scaling 组以使用多个可用性区域，可以非常简单地为此架构启用高可用性。ASG 将自动平衡负载，因此您实际上不需要为每个 AZ 指定实例。Web 层的体系结构如下所示：



正确：正确的答案是“修改 Auto Scaling 组以在两个可用区中的每个可用区中使用四个实例”。

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

错误：“创建一个在两个区域中每个区域使用四个实例的 Auto Scaling 组”是错误的，因为 **EC2 Auto Scaling 不支持多个区域**. 错误：“创建可用于在另一个区域中快速创建更多实例的 Auto Scaling 模板”是错误的，因为 **EC2 Auto Scaling 不支持多个区域**. 错误：“创建一个在两个子网中的每个子网中使用四个实例的 Auto Scaling 组”是错误的，因为这些子网可能位于同一可用区中.

参考文献：

<https://aws.amazon.com/ec2/autoscaling/>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-autoscaling/>

**Q4.** 公司运行基于内部浏览器的应用程序. 该应用程序在 **Application Load Balancer** 后面的 **Amazon EC2** 实例上运行.

实例在多个可用区中的 **Amazon EC2 Auto Scaling** 组中运行. **Auto Scaling** 组在工作时间内最多可扩展 20 个实例，而在一夜之间最多可扩展到 2 个实例. 工作人员抱怨说，尽管一天早晨运行良好，但该应用程序在一天开始时运行缓慢.

应该如何改变规模，以解决员工的投诉并将成本降至最低？

- A. 实施一项计划的行动，以在办公室开放之前不久将所需的容量设置为 20
- B. 执行以较低的 CPU 阈值触发的逐步扩展操作，并缩短冷却时间
- C. 实施在较低的 CPU 阈值下触发的目标跟踪动作，并缩短冷却时间**
- D. 实施预定的行动，在办事处开业前不久将最小和最大容量设置为 20

答案:A

淘宝：国际认证大师 微信：ANYPASS

尽管这听起来像是计划动作的好用例，但无论实际需求如何，使用计划动作的两个答案都将运行 20 个实例. 更具成本效益的更好选择是使用**目标跟踪操作**，该操作在较低的 CPU 阈值处触发. 使用此解决方案，可在 CPU 利用率达到影响性能的点之前进行扩展. 这将在解决性能问题的同时将成本降至最低. **使用缩短的冷却时间还可以更快地终止不需要的实例**，从而进一步降低成本.

正确：“实施在较低的 CPU 阈值下触发的目标跟踪操作，并减少冷却时间”是正确的答案.

错误：“在办公室开业之前立即执行将所需容量设置为 20 的计划动作”是不正确的，因为这不是最具成本效益的选择. 请注意，您可以为计划的操作选择最小值，最大值或所需的值.

不正确：“立即实施将最小和最大容量设置为 20 的计划操作”不正确，因为这不是最具成本效益的选择. 请注意，您可以为计划的操作选择最小值，最大值或所需的值. 不正确：“实施在较低的 CPU 阈值下触发的步进扩展操作，并减少冷却时间”是不正确的，**因为在大多数情况下，AWS 建议您使用目标跟踪来代替步进扩展.**

参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-autoscaling/>

**Q5.** 解决方案架构师正在设计一种解决方案，以访问图像目录并为用户提供提交自定义图像请求的能力.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

图像定制参数将存在于发送到 AWS API Gateway API 的任何请求中。定制图像将按需生成，用户将获得一个链接，他们可以单击链接以查看或下载其定制图像。

该解决方案必须高度可用以查看和自定义图像，满足这些要求的最经济有效的解决方案是什么？

A. 使用 Amazon EC2 实例将原始图像处理为请求的自定义。

将原始图像和经过处理的图像存储在 Amazon S3 中。

在 EC2 实例之前配置 Elastic Load Balancer。

B. 使用 AWS Lambda 将原始图像处理为请求的自定义。

将原始图像和经过处理的图像存储在 Amazon S3 中。

使用 S3 存储桶作为 origin 配置 Amazon CloudFront 分配。

C. 使用 AWS Lambda 将原始图像处理为请求的自定义。

将原始图像存储在 Amazon S3 中，将经过处理的图像存储在 Amazon DynamoDB 中。

在 Amazon EC2 实例之前配置 Elastic Load Balancer。

D. 使用 Amazon EC2 实例将原始图像处理为请求的自定义。

将原始图像存储在 Amazon S3 中，将经过处理的图像存储在 Amazon DynamoDB 中。

使用 S3 存储桶作为源配置 Amazon CloudFront 分配。

答案:B

提出的所有解决方案都是高度可用的。必须满足的关键要求是该解决方案应具有成本效益，并且您必须选择最具成本效益的选项。因此，**最好消除诸如 Amazon EC2 和 ELB 之类的服务，因为即使不使用它们也需要持续的成本。**

**相反，应使用完全无服务器的解决方案 AWS Lambda, Amazon S3 和 CloudFront 是满足这些要求的最佳服务。正确：“使用 AWS Lambda 将原始图像处理为所请求的自定义。将原始图像和处理后的图像存储在 Amazon S3 中。将以 S3 存储桶为源的 Amazon CloudFront 分配配置为正确的答案”。错误：“使用 Amazon EC2 实例将原始图像处理为请求的自定义。将原始图像和经过处理的图像存储在 Amazon S3 中。在 EC2 实例之前配置 Elastic Load Balancer”是不正确的。这不是最具成本效益的选项，因为 ELB 和 EC2 实例即使不使用也会产生费用。不正确：“使用 AWS Lambda 操纵原始图像请求的自定义。将原始图像存储在 Amazon S3 中，将经过处理的图像存储在 Amazon DynamoDB 中。在 Amazon EC2 实例前面配置弹性负载均衡器”是不正确的。这不是最具成本效益的选项，因为 ELB 即使不使用也会产生费用。而且，Amazon DynamoDB 在运行时会产生 RCU / WCU，而在没有运行时会产生 RCU / WCU 存储图像的最佳选择。这不是最具成本效益的选择，因为即使不使用 ELB 和 EC2 实例也会产生成本。错误：“使用 AWS Lambda 将原始图像处理为请求的自定义。将原始图像存储在 Amazon S3 中，将处理后的图像存储在 Amazon DynamoDB 中。在 Amazon EC2 实例之前配置 Elastic Load Balancer”。这不是最具成本效益的选择，因为 ELB 即使不使用也会产生费用。此外，Amazon DynamoDB 在运行时会产生 RCU / WCU，这不是存储图像的最佳选择。这不是最具成本效益的选择，因为即使不使用 ELB 和 EC2 实例也会产生成本。错误：“使用 AWS Lambda 将原始图像处理为请求的自定义。将原始图像存储在 Amazon S3 中，将处理后的图像存储在 Amazon DynamoDB 中。在 Amazon EC2 实例之前配置 Elastic Load Balancer”。这不是最具成本效益的选择，因为 ELB 即使不使用也会产生费用。此外，Amazon DynamoDB 在运行时会产生 RCU / WCU，这不是存储图像的最佳选择。错误：“使用 Amazon EC2 实例将原始图像处理到请求的自定义中。将原始图像存储在 Amazon S3 中，将处理后的图像存储在 Amazon DynamoDB 中。将以 S3 存储桶为源的 Amazon CloudFront 分配配置为错误”。这不是最具成本效益的选择，因为即使不使用 EC2 实例也会产生成本参考文献：**

<https://aws.amazon.com/serverless/>

使用我们特定于考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

**Q6.** 一家自行车共享公司正在开发一种多层次体系结构，以在高峰运营时间跟踪其自行车的位置。该公司希望在其现有的分析平台中使用这些数据点。解决方案架构师必须确定最可行的多层次选项来支持该体系结构。必须可以从 REST API 访问数据点。哪项操作符合存储和检索位置数据的这些要求？

- A. 将 Amazon Athena 与 Amazon S3 结合使用
- B. 将 Amazon API Gateway 与 AWS Lambda 结合使用
- C. 将 Amazon QuickSight 与 Amazon Redshift 结合使用
- D. 将 Amazon API Gateway 与 Amazon Kinesis Data Analytics 结合使用

答案:B

关键字：现有分析平台中的数据点+必须从 REST API 中访问数据点+在高峰时段跟踪自行车的位置他们已经拥有一个分析平台，A（Athena）和 D（Kinesis Data Analytics）已淘汰竞争激烈的 S3 和 APT 网关支持 REST API。现在 B 和 C 都在比赛中。C 将不支持 REST API。因此，根据以下详细信息，答案应为 B。

淘宝：国际认证大师 微信：ANYPASS

现在，如果我们谈论数据类型，我们正在谈论他们的自行车的 GEO 位置数据。API 网关将支持 REST API。因此，确切的解决方案应该是带有 AWS Lambda 的 API 网关以及 Amazon Kinesis Data Analytics（假定已使用）。

正确：“将 Amazon API Gateway 与 AWS Lambda 一起使用”是正确的答案。错误：“将 Amazon Athena 与 Amazon S3 一起使用”是不正确的，因为他们已经具有分析平台。

错误：“将 Amazon QuickSight 与 Amazon Redshift 一起使用”是不正确的。这不支持 REST API。

错误：“将 Amazon API Gateway 与 Amazon Kinesis Data Analytics 结合使用”是不正确的，因为他们已经具有分析平台。

参考文献：

<https://aws.amazon.com/api-gateway/>

<https://aws.amazon.com/lambda/>

<https://aws.amazon.com/kinesis/data-analytics/>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-athena/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

**Q7.** 解决方案架构师正在多个 Amazon EC2 实例上部署分布式数据库。数据库将所有数据存储在多个实例上，因此它可以承受一个实例的丢失。该数据库需要具有延迟和吞吐量的块存储，以支持每台服务器每秒几百万个事务。

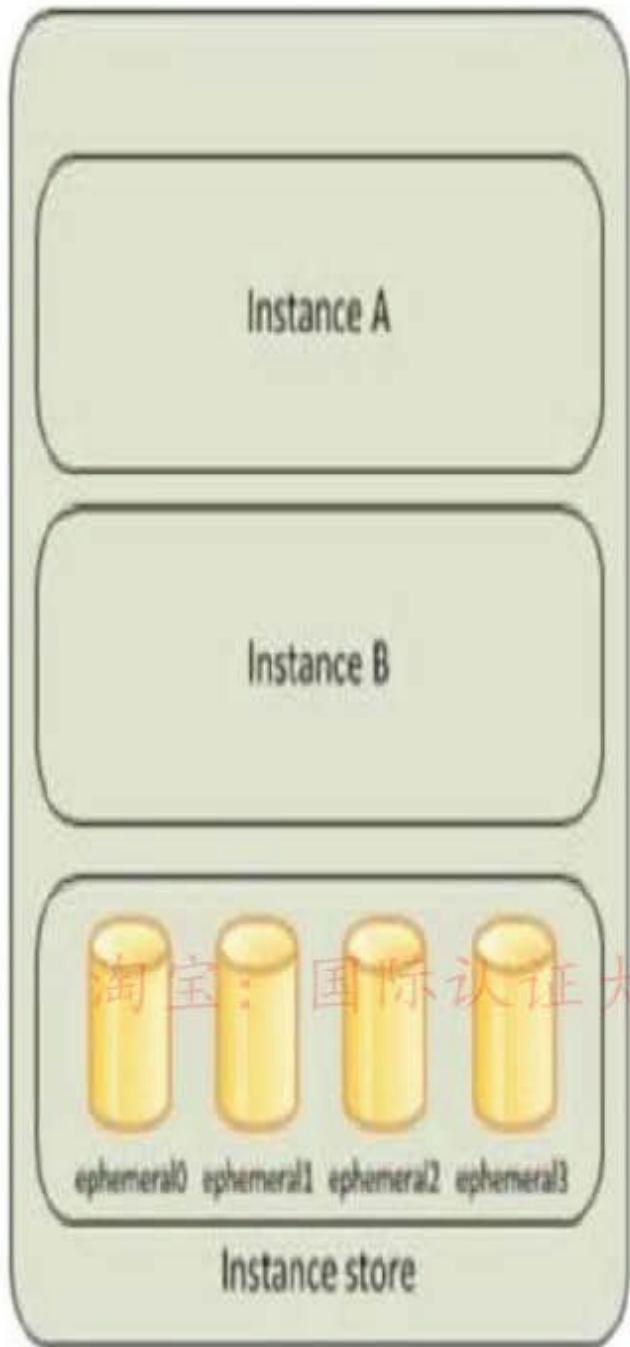
解决方案架构师应使用哪种存储解决方案？

- A. 亚马逊 EBS
- B. Amazon EC2 实例存储
- C. Amazon EFS
- D. 亚马逊 S3

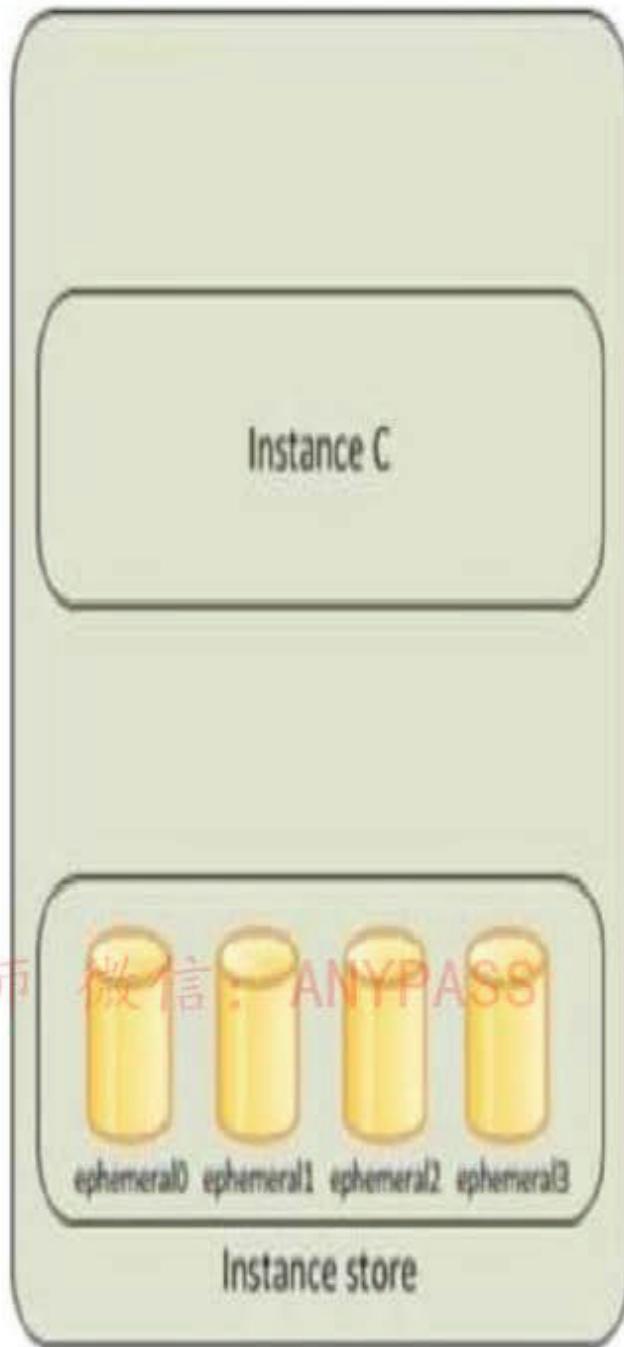
答案：**B**

实例存储为您的实例提供临时的块级存储。该存储位于物理上连接到主机的磁盘上。实例存储非常适合用于临时存储经常更改的信息（例如缓冲区，缓存，暂存数据和其他临时内容），或者用于跨实例实例复制的数据（例如负载均衡的 Web 服务器池）。

淘宝：国际认证大师 微信：ANYPASS



Host Computer 1



Host Computer 2

某些实例类型使用 NVMe 或基于 SATA 的固态驱动器 (SSD) 来提供较高的随机 I/O 性能。当您需要具有非常低的延迟的存储，但是当实例终止时您不需要数据持久化或者可以利用容错架构时，这是一个很好的选择。

在这种情况下，数据已复制且具有容错能力，因此提供所需性能级别的最佳选择是使用实例存储卷。正确：“Amazon EC2 实例存储”是正确的答案。错误：“Amazon EBS”不正确。弹性块存储 (EBS) 是一种块存储设备，但是由于数据是分布式的且具有容错能力，因此，使用实例存储是一种更好的性能选择。

错误：“Amazon EFS”不正确，因为 EFS 不是块设备，它是使用 NFS 协议访问的文件系统。

错误：“Amazon S3”不正确，因为 S3 是基于对象的存储系统，而不是基于块的存储系统。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html> 使用我们针对考试的备忘单来节省时间：

[https://digitalcloud.training/certification-training/aws-solutions-architect- associate / compute / amazon-ebs /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate / compute / amazon-ebs /)

Q8. 解决方案架构师需要确保从 VPC 中的 Amazon EC2 实例对 Amazon DynamoDB 的 API 调用不会遍历 Internet.

解决方案架构师应该怎么做才能做到这一点？（选择两个）

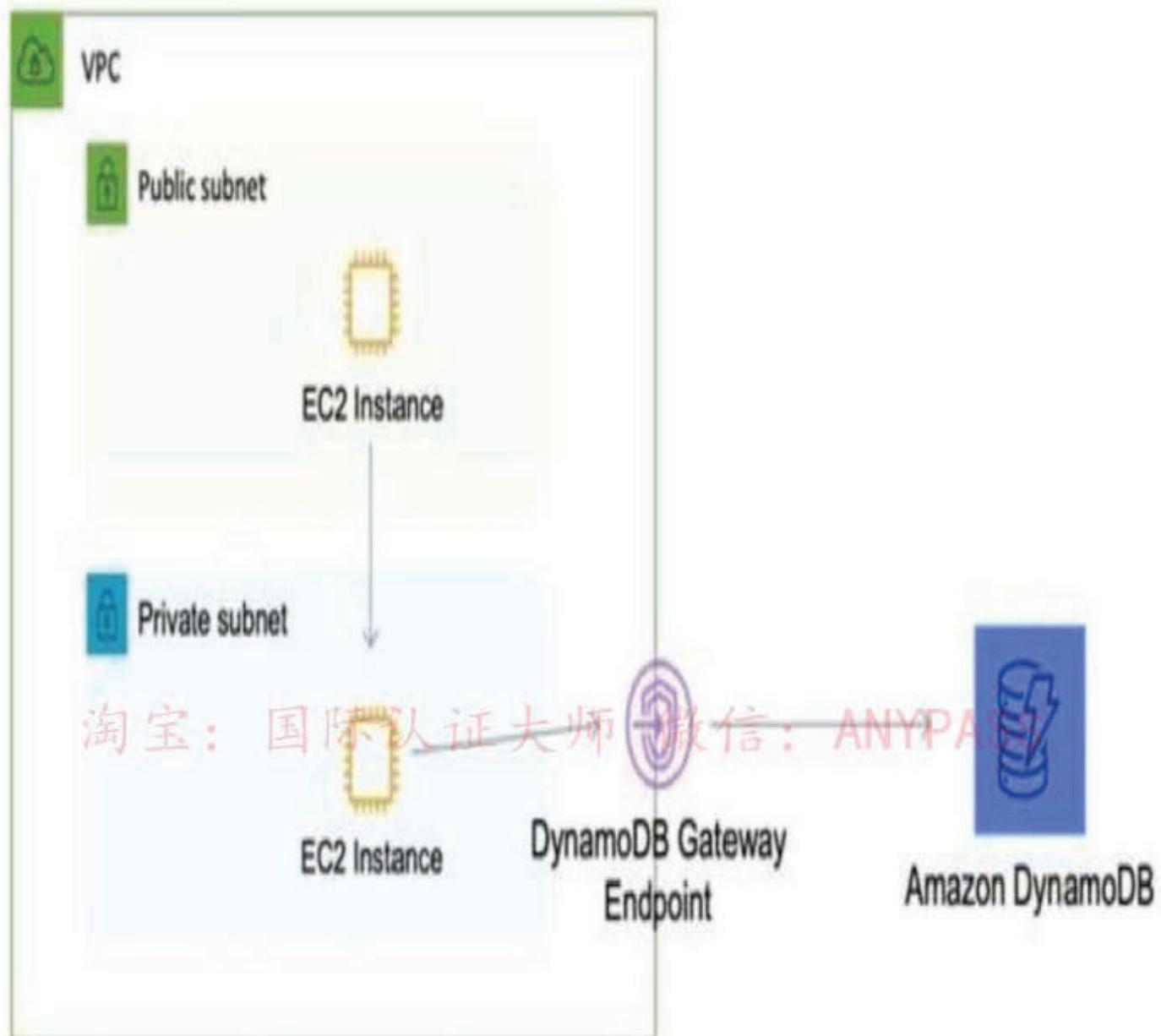
- A.为端点创建一个路由表条目
- B.为 DynamoDB 创建网关端点
- C.创建一个使用端点的新 DynamoDB 表
- D.在 VPC 的每个子网中为端点创建一个 ENI
- E.在默认安全组中创建一个安全组条目以提供访问权限

答案:AB

Amazon DynamoDB 和 Amazon S3 支持网关终端节点，不支持接口终端节点。使用网关端点，您可以在 VPC 中创建端点，附加允许访问服务的策略，然后指定路由表以在其中创建路由表条目。

淘宝：国际认证大师 微信：ANYPASS

## Default VPC



## Route Table

Destination	Target
<code>pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)</code>	<code>vpce-ID</code>

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

正确：“为端点创建路由表条目”是正确的答案。正确：“为 DynamoDB 创建网关端点”也是正确的答案。错误：“创建使用端点的新 DynamoDB 表”是错误的，因为没有必要创建新的 DynamoDB 表。  
错误：“在 VPC 的每个子网中为端点创建 ENI”不正确，因为接口端点而不是网关端点使用了 ENI。  
错误：“在 VPC 和 DynamoDB 之间创建 VPC 对等连接”不正确，因为您无法在 VPC 和公共 AWS 服务之间创建 VPC 对等连接，因为公共服务不在 VPC 之外。

参考文献：

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

Q9. 解决方案架构师正在设计一个 Web 应用程序，该应用程序将在 Application Load Balancer (ALB) 之后的 Amazon EC2 实例上运行。

该公司严格要求该应用程序具有抵御恶意 Internet 活动和攻击的能力，并防范新的常见漏洞和暴露。

解决方案架构师应该建议什么？

- A. 以 ALB 终端节点为源利用 Amazon CloudFront
- B. 为 AWS WAF 部署适当的托管规则并将其与 ALB 关联
- C. 订阅 AWS Shield Advanced 并确保常见漏洞和暴露被阻止
- D. 配置网络 ACL 和安全组以仅允许端口 80 和 443 访问 EC2 实例

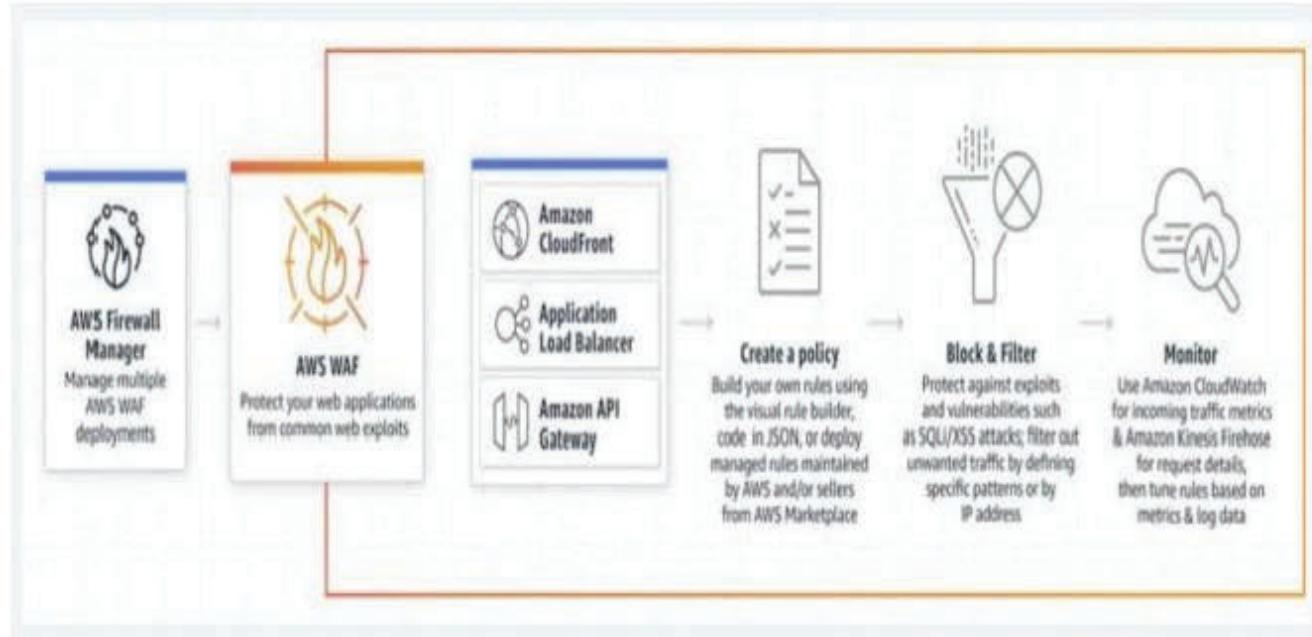
答案：B

淘宝：国际认证大师 微信：ANYPASS

您可以将 AWS WAF 作为 CDN 解决方案的一部分部署在 Amazon CloudFront 上，也可以将应用程序负载均衡器部署在 EC2 上运行的 Web 服务器或原始服务器的前端，也可以将 API 部署在 Amazon API Gateway 中。

易于部署和维护

AWS WAF 易于部署和保护部署在 CDN 解决方案中的 Amazon CloudFront 上，部署在所有原始服务器前面的 Application Load Balancer 或 API 的 Amazon API Gateway 上的应用程序。无需部署其他软件，无需配置 DNS 配置，无需管理 SSL / TLS 证书，也无需进行反向代理设置。借助 AWS Firewall Manager 集成，您可以集中定义和管理规则，并在需要保护的所有 Web 应用程序中重用它们。



正确：“为 AWS WAF 部署适当的托管规则并将其与 ALB 关联”是正确的答案。

不正确：“将 Amazon CloudFront 以 ALB 终端节点为源”不正确，因为它不满足安全性要求。

错误：“订阅 AWS Shield Advanced 并确保阻止常见漏洞和暴露”是错误的，因为这将支持 ELB 错误：“将网络 ACL 和安全组配置为仅允许端口 80 和 443 访问 EC2 实例”不正确，因为“新的常见漏洞和披露”

参考文献：淘宝：国际认证大师 微信：ANYPASS

<https://aws.amazon.com/waf/>

<https://aws.amazon.com/shield/>

<https://aws.amazon.com/shield/features/>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-waf-and-shield/>

Q10. 过去几年，一家公司一直将分析数据存储在 Amazon RDS 实例中。该公司要求解决方案架构师找到一种解决方案，允许用户使用 API 来访问此数据。预期该应用程序将经历一段时间的不活动状态，但可能会在几秒钟内收到大量流量。解决方案架构师应建议哪种解决方案？

- A. 设置一个 Amazon API Gateway 并使用 Amazon ECS.
- B. 设置一个 Amazon API Gateway 并使用 AWS Elastic Beanstalk.
- C. 设置 Amazon API Gateway 并使用 AWS Lambda 函数
- D. 设置 Amazon API Gateway 并将 Amazon EC2 与 Auto Scaling 一起使用

答案:C

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

这个问题只是在要求您为规定的要求制定出最佳的计算服务。关键要求是计算服务应适用于需求范围很广的工作负载，从无请求到大流量突发。AWS Lambda 是一种理想的解决方案，因为您仅在发出请求时才付费，并且可以轻松扩展以容纳大量流量。Lambda 与 API Gateway 和 Amazon RDS 均能很好地工作。

正确：“设置 Amazon API Gateway 并使用 AWS Lambda 函数”是正确的答案。

错误：“设置 Amazon API Gateway 并使用 Amazon ECS”是不正确的，因为 Lambda 更适合此用例，因为流量模式是高度动态的。错误：“设置 Amazon API 网关并使用 AWS Elastic Beanstalk”是不正确的，因为流量模式是高度动态的，因此 Lambda 更适合此用例。错误：“设置 Amazon API 网关并将 Amazon EC2 与 Auto Scaling 一起使用”是不正确的，因为流量模式是高度动态的，因此 Lambda 更适合此用例。

参考文献：

<https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

Q11. 公司的 Web 应用程序正在使用多个 Linux Amazon EC2 实例，并将数据存储在 Amazon EBS 卷上。

该公司正在寻找一种解决方案，以在出现故障的情况下提高应用程序的弹性，并提供符合原子性、一致性、隔离性和耐用性（ACID）的存储。

解决方案架构师应该怎么做才能满足这些要求？

A. 在每个可用区中的 EC2 实例上启动应用程序。

将 EBS 卷附加到每个 EC2 实例。

B. 使用跨多个可用区的 Auto Scaling 组创建一个 Application Load Balancer。

在每个 EC2 实例上安装一个实例存储。

C. 使用跨多个可用区的 Auto Scaling 组创建一个 Application Load Balancer。

将数据存储在 Amazon EFS 上，并在每个实例上安装一个目标。

D. 使用跨多个可用区的 Auto Scaling 组创建一个 Application Load Balancer。

使用 Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) 存储数据。

答案：C

为了提高应用程序的弹性，解决方案架构师可以使用 Auto Scaling 组根据需要在多个可用性区域中启动和终止实例。应用程序负载平衡器 (ALB) 可用于将流量定向到在 EC2 实例上运行的 Web 应用程序。

最后，Amazon Elastic File System (EFS) 通过提供可以由来自多个可用性区域的多个 EC2 实例安装的共享文件系统，可以帮助提高应用程序的弹性。

正确：“使用跨多个可用区的 Auto Scaling 组创建应用程序负载平衡器。在 Amazon EFS 上存储数据并在每个实例上安装目标”是正确的答案。

错误：“在每个可用区的 EC2 实例上启动应用程序。将 EBS 卷附加到每个 EC2 实例”是不正确的，因为 EBS 卷是单点故障，无法与其他实例共享。

错误：“使用跨多个可用区的 Auto Scaling 组创建应用程序负载均衡器。在每个 EC2 实例上安装实例存储”是不正确的，因为实例存储是临时数据存储。这意味着在断电时数据会丢失。同样，实例存储不能在实例之间共享。

错误：“使用跨多个可用区的 Auto Scaling 组创建应用程序负载平衡器，使用 Amazon S3 一次区域不频繁访问（S3 One Zone-IA）存储数据”是不正确的，因为与此 S3 层相关联的数据检索费用，它不适用于应用程序文件的存储层。

参考文献：

<https://docs.aws.amazon.com/efs/>

使用我们特定于考试的备忘单节省时间：

[https://digitalcloud.training/certification-training/aws-solutions-architect-associate / storage / amazon-efs /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/)

**Q12.** 公司有一个调用 AWS Lambda 函数的应用程序。最近的代码审查发现源代码中存储了数据库凭据。需要从 Lambda 源代码中删除数据库凭据。然后必须安全地存储凭据并不断对其进行轮换以满足安全策略要求。

解决方案架构师应建议哪些以满足这些要求？

A. 将密码存储在 AWS CloudHSM 中。

将 Lambda 函数与一个角色相关联，该角色可以从 CloudHSM 检索给定其密钥 ID 的密码。

B. 将密码存储在 AWS Secrets Manager 中。

将 Lambda 函数与一个角色相关联，该角色可以从 Secrets Manager 中获取给定其秘密 ID 的密码。

C. 将数据库密码移至与 Lambda 函数关联的环境变量。

执行时从环境变量中检索密码。

D. 将密码存储在 AWS Key Management Service (AWS KMS) 中。

将 Lambda 函数与一个角色相关联，该角色可以根据给定的密钥 ID 从 AWS KMS 检索密码。

答案：**B**

淘宝：国际认证大师 微信：ANYPASS

**Q13.** 解决方案架构师需要在 Amazon S3 存储桶中使用静态网站。解决方案架构师需要确保在意外删除的情况下可以恢复数据。

哪个动作可以完成此任务？

A. 启用 Amazon S3 版本

B. 启用 Amazon S3 智能分层。

C. 启用 Amazon S3 生命周期策略

D. 启用 Amazon S3 跨区域复制。

答案：**A**

对象版本控制是将对象的多个变体保留在同一 Amazon S3 存储桶中的一种方法。版本控制可以从意外的用户操作和应用程序故障中恢复。您可以使用版本控制来保留、检索和还原存储在 Amazon S3 存储桶中的每个对象的每个版本。

正确：“启用 Amazon S3 版本控制”是正确的答案。错误：“启用 Amazon S3 智能分层”是不正确的。这是一个存储类，可以根据使用模式在频繁访问和不频繁访问类之间自动移动数据。

错误：“启用 Amazon S3 生命周期策略”不正确。S3 生命周期策略是一组规则，这些规则定义了适用于 S3 对象组的操作，例如将对象过渡到另一个存储类。

不正确：“启用 Amazon S3 跨区域复制”不正确，因为这是用于将对象复制到不同区域的。CRR 依赖于版本控制，这是防止意外删除所必需的功能。

参考文献：

<https://d0.awsstatic.com/whitepapers/protecting-s3-against-object-deletion.pdf> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-s3 />

#### Q14. 一家公司正在本地管理健康记录。

公司必须无限期地保留这些记录，一旦存储了记录就禁止对记录进行任何修改，并仔细审核各个级别的访问权限。首席技术官（CTO）感到担心，因为已经有数百万条记录未被任何应用程序使用，并且当前的基础架构空间不足。CTO 已要求解决方案架构师设计一种解决方案，以移动现有数据并支持将来的记录。

解决方案架构师可以推荐哪些服务来满足这些要求？

A. 使用 AWS DataSync 将现有数据移至 AWS.

使用 Amazon S3 存储现有数据和新数据。

启用 Amazon S3 对象锁定，并为 AWS CloudTrail 启用 数据事件。

B. 使用 AWS Storage Gateway 将现有数据移至 AWS.

使用 Amazon S3 存储现有数据和新数据。

启用 Amazon S3 对象锁定，并通过管理事件启用 AWS CloudTrail.

C. 使用 AWS DataSync 将现有数据移至 AWS.

使用 Amazon S3 存储现有数据和新数据。

启用 Amazon S3 对象锁定，并通过管理事件启用 AWS CloudTrail.

D. 使用 AWS Storage Gateway 将现有数据移至 AWS.

使用 Amazon Elastic Block Store (Amazon EBS) 存储现有数据和新数据。

启用 Amazon S3 对象锁定并启用 Amazon S3 服务器访问日志记录。

答案：A

原始答案 B，现更正为 A

关键字：移动现有数据并支持将来的记录+各个级别的粒度审核访问

使用 AWS DataSync 将现有数据迁移到 Amazon S3，然后使用 AWS Storage Gateway 的 File Gateway 配置保留对已迁移数据的访问权限，并保留来自基于本地文件的应用程序的持续更新。

需要一种解决方案来移动现有数据并支持将来的记录 = AWS DataSync 应该用于迁移。

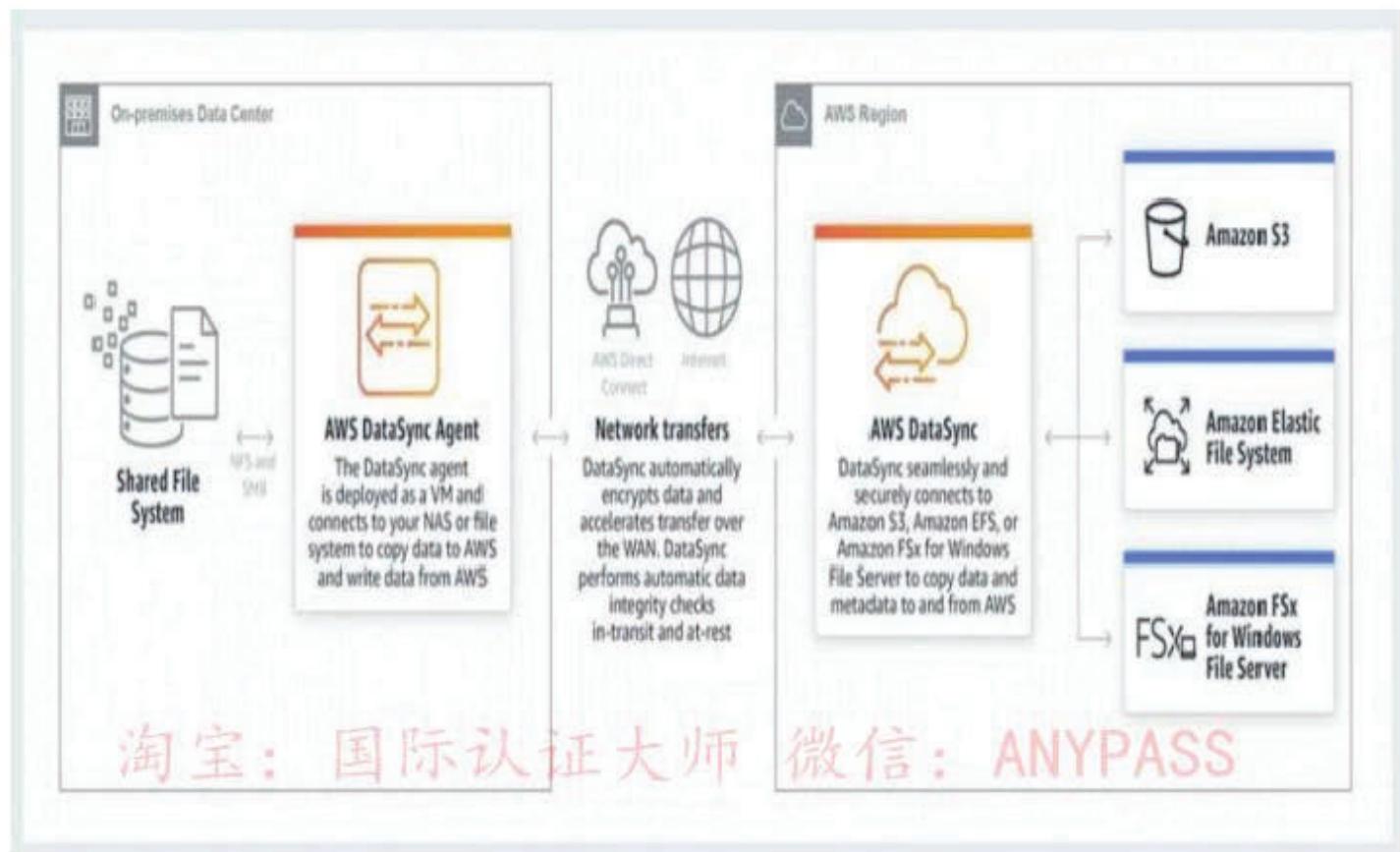
需要所有级别的精细审核访问权限 = CloudTrail 中应使用 数据事件，默认情况下启用管理事件。

正确：“使用 AWS DataSync 将现有数据移至 AWS. 使用 Amazon S3 存储现有数据和新数据. 启用 Amazon S3 对象锁定并为 AWS CloudTrail 启用数据事件”是正确的答案。

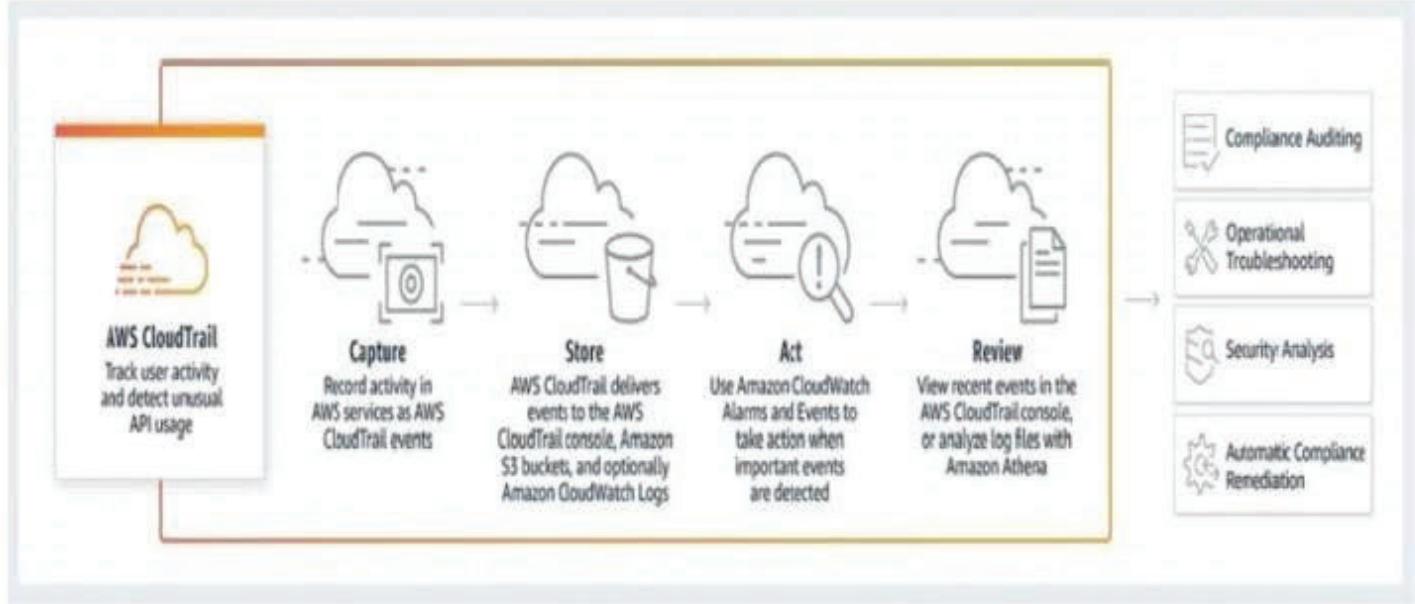
错误：“使用 AWS Storage Gateway 将现有数据移动到 AWS. 使用 Amazon S3 存储现有数据和新数据. 启用 Amazon S3 对象锁定并通过管理事件启用 AWS CloudTrail”是错误的，因为“当前基础架构空间不足”：“使用 AWS DataSync 将现有数据移至 AWS. 使用 Amazon S3 存储现有数据和新数据. 启用 Amazon S3 对象锁定并通过管理事件启用 AWS CloudTrail.” 错误，因为“默认情

况下启用了管理事件”不正确：“使用 AWS Storage Gateway 将现有数据移动到 AWS. 使用 Amazon Elastic Block Store (Amazon EBS) 存储现有数据和新数据. 启用 Amazon S3 对象锁定并启用 Amazon S3 服务器访问日志记录.” 不正确，因为“当前基础结构空间不足”

### AWS DataSync 的工作方式



### AWS CloudTrail 的工作方式



参考文献：

<https://aws.amazon.com/datasync/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>  
<https://aws.amazon.com/cloudtrail/>  
<https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

使用我们特定于考试的备忘单节省时间：淘宝 国际认证大师 微信：ANYPASS  
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

**Q15.** 一家公司目前正在运行由 Amazon RDS MySQL 数据库支持的 Web 应用程序。它具有每天运行且未加密的自动备份。安全审核要求对将来的备份进行加密，而将未加密的备份销毁。在销毁旧备份之前，公司将至少进行一次加密备份，应如何做才能为以后的备份启用加密？

- A. 为存储备份的 Amazon S3 存储桶启用默认加密。
- B. 修改数据库配置的备份部分以切换“启用加密”复选框。
- C. 创建数据库快照。  
将其复制到加密的快照。  
从加密的快照还原数据库。
- D. 在 MySQL 的 RDS 上启用加密的只读副本。  
将加密的只读副本提升为主数据库。  
删除原始数据库实例。

答案:C

Amazon RDS 使用快照进行备份。仅当数据库已加密时，快照才会在创建时进行加密，并且只能在首次创建数据库时选择加密。在这种情况下，数据库以及快照均未加密。但是，您可以创建快照

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

的加密副本。您可以使用该快照进行还原，该快照将创建一个启用了加密的新数据库实例。从那时起，将为所有快照启用加密。

正确：“创建数据库的快照，将其复制到加密的快照，从加密的快照还原数据库”是正确的答案。错误：“无法在 RDS 上为 MySQL 启用加密的只读副本，将加密的只读副本升级为主副本，删除原始数据库实例”是错误的，因为您无法从未加密的主服务器创建加密的只读副本。

错误：由于无法为现有数据库添加加密，因此“修改数据库配置的备份部分以切换“启用加密”复选框”是错误的。错误：“对存储备份的 Amazon S3 存储桶启用默认加密”是不正确的，因为您无权访问存储快照的 S3 存储桶。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / database / amazon-rds />

**Q16.** 客户端报告他们希望查看其帐户中对 AWS 资源进行的任何更改的审核日志。

客户可以做些什么来实现这一目标？

- A. 在他们拥有的服务上设置 Amazon CloudWatch 监视器
- B. 启用将 AWS CloudTrail 日志传递到 Amazon S3 存储桶
- C. 使用 Amazon CloudWatch Events 解析日志
- D. 使用 AWS OpsWorks 来管理其资源

答案：**B**

淘宝：国际认证大师 微信：ANYPASS

可以创建 CloudTrail 跟踪，该跟踪将日志文件传递到 Amazon S3 存储桶。

**Q17.** 在专用子网中运行的应用程序访问 Amazon DynamoDB 表。有一个安全要求，即数据永远都不会离开 AWS 网络。

应如何满足此要求？

- A. 在 DynamoDB 上配置网络 ACL 以将流量限制到专用子网
- B. 使用 AWS KMS 密钥启用静态 DynamoDB 加密
- C. 添加一个 NAT 网关并在专用子网上配置路由表
- D. 为 DynamoDB 创建 VPC 端点并配置端点策略

答案：**D**

提示：专用子网=VPC 端点

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups <small>https://aws.amazon.com/cn/dynamodb/dax/</small>	VPC Endpoint Policies

Q18. 正在创建一个三层应用程序来托管小新闻文章。该应用程序有望为数百万用户提供服务。发生重大新闻时，该站点必须处理非常大的流量峰值，而又不会显著影响数据库性能。

哪种设计可以在最小化成本的同时满足这些要求？

- A. 使用 Auto Scaling 组增加交付 Web 应用程序的 Amazon EC2 实例的数量
- B. 使用 Auto Scaling 组增加交付数据库的 Amazon RDS 实例的大小
- C. 使用 Amazon DynamoDB 高度一致的读取来调整流量的增长
- D. 使用 Amazon DynamoDB Accelerator (DAX) 将读取操作缓存到数据库

答案:D

**DAX 具有内存缓存。**如果发生重大新闻，搜索的大多数用户将寻找完全相同的事物。话虽如此，请求将首先查询内存缓存，而无需直接从数据库中获取数据。

Q19. 在审查业务应用程序时，解决方案架构师使用由业务用户构建并在用户桌面上运行的关系数据库来识别关键应用程序。为了降低业务中断的风险，解决方案架构师希望将应用程序迁移到 AWS 中的高可用性多层解决方案。

解决方案架构师应该怎么做才能对业务造成最少的破坏？

- A. 创建应用程序代码的导入包以上传到 AWS Lambda，并包括一个用于创建另一个 Lambda 函数的功能，以将数据迁移到 Amazon RDS 数据库
- B. 创建用户桌面的映像，使用 VM Import 将其迁移到 Amazon EC2，并将 EC2 实例放置在 Auto Scaling 组中
- C. 在 Application Load Balancer 和 Amazon RDS Multi-AZ DB 实例后面的 AWS 上预先运行新的 Amazon EC2 实例

D. 使用 AWS DMS 将后端数据库迁移到 Amazon RDS Multi-AZ 数据库实例.

**将应用程序代码迁移到 AWS Elastic Beanstalk**

答案:D

Q20. 一家公司在具有明确定义的访问模式的 Amazon S3 存储桶中存储了数千个文件. 在最初的 30 天内, 应用程序每天多次访问文件. 在接下来的 90 天内很少访问文件. 之后, 将不再访问文件. 在最初的 120 天内, 访问这些文件的时间绝不会超过几秒钟.

应该为 S3 对象使用哪种生命周期策略, 以根据访问模式将成本降至最低?

A. 前 30 天使用 Amazon S3 Standard-Infrequent Access (S3 Standard-IA) 存储. 然后在接下来的 90 天内将文件移至 GLACIER 存储类. 之后允许数据过期.

B. 前 30 天使用 Amazon S3 Standard 存储. 然后在接下来的 90 天内将文件移动到 Amazon S3 Standard-Infrequent Access (S3 Standard-IA). 之后允许数据过期.

C. 前 30 天使用 Amazon S3 Standard 存储. 然后在接下来的 90 天内将文件移至 GLACIER 存储类. 之后允许数据过期.

D. 前 30 天使用 Amazon S3 Standard-Infrequent Access (S3 Standard-IA). 之后, 将数据移至 GLACIER 存储类, 该类将被自动删除.

答案:B

提到他们需要在 120 天内几秒钟内访问数据.

Q21. 公司每天晚上都会创建关键业务 3D 图像. 图像在每个星期五进行批处理, 并且需要 48 小时不间断地完成.

在这种情况下, 什么是最具成本效益的 Amazon EC2 定价模型?

A. 按需实例

B. 预定的预留实例

C. 预留实例

D. 竞价型实例

答案:B

通过计划的预留实例 (计划的实例), 您可以购买以一年, 一年, 每天, 每周或每月为基础的, 具有指定开始时间和持续时间的容量预留. 您预先预留了容量, 以便知道在需要时可用. 即使您不使用实例, 也要为实例安排的时间付费.

对于不是连续运行但可以按计划运行的工作负载, 计划实例是不错的选择. 例如, 您可以将“调度实例”用于在工作时间运行的应用程序或在周末运行的批处理. 正确: “预定的预留实例”是正确的答案. 不正确: “标准预留实例”不正确, 因为工作负载每天仅运行 4 个小时, 这会更加昂贵.

不正确: “按需实例”是不正确的, 因为由于没有折扣, 这将更加昂贵.

错误: “Spot Instances”不正确, 因为一旦启动工作负载就无法中断. 如果需要竞价价格或容量, 可以使用竞价型实例终止工作负载.

参考文献:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html> 使用我们针对考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

Q22. 应用程序生成操作活动的审核日志。遵从性要求要求应用程序将日志保留 5 年。

如何满足这些要求？

- A. 将日志保存在 Amazon S3 存储桶中，并在存储桶上启用多因素身份验证删除（MFA Delete）。
- B. 将日志保存在 Amazon EFS 卷中，并使用该卷的网络文件系统版本 4（NFSv4）锁定。
- C. 将日志保存在 Amazon Glacier 保管库中，并使用保管库锁定功能。
- D. 将日志保存在 Amazon EBS 卷中，并每月拍摄一次快照。

答案:C

能够长期存储关键任务数据的 Amazon Glacier 添加了 Vault Lock。这项新功能使您可以使用旨在支持此类长期记录保留的各种合规性控件来锁定保管库。

Q23. 解决方案架构师正在创建在 Amazon VPC 中运行的应用程序，该应用程序需要访问 AWS Systems Manager 参数存储。网络安全规则禁止任何目的地为 0.0.0.0/0 的路由表条目。

哪些基础架构新增功能将允许在满足要求的同时访问 AWS 服务？

- 淘宝：国际认证大师 微信：ANYPASS
- A. VPC 对等
  - B. NAT 实例
  - C. NAT 网关
  - D. AWS PrivateLink

答案:D

要从 Amazon VPC 将消息发布到 Amazon SNS 主题，请创建接口 VPC 终端节点。然后，您可以将消息发布到 SNS 主题，同时将使用 VPC 管理的网络中的流量保持在该范围内。这是最安全的选项，因为流量不需要遍历 Internet。

正确：“使用 AWS PrivateLink”是正确的答案。错误：“使用 Internet 网关”不正确。公共子网中的实例使用 Internet 网关访问 Internet，这比 VPC 端点安全性低。错误：“使用代理实例”不正确。代理实例也将使用公共 Internet，因此其安全性低于 VPC 端点。

不正确：“使用 NAT 网关”不正确。专用子网中的实例使用 NAT 网关来访问 Internet，这比 VPC 端点的安全性低。

参考文献:

<https://docs.aws.amazon.com/sns/latest/dg/sns-vpc-endpoint.html> 使用我们针对考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

**Q24.** 在 AWS 上运行的照片共享网站允许用户生成存储在 Amazon S3 中的照片的缩略图。Amazon DynamoDB 表维护照片的位置，如果不小心删除了缩略图，则可以轻松地从原始照片重新创建缩略图。

缩略图应如何存储以确保最低成本？

- A. 具有跨区域复制的 Amazon S3 标准不频繁访问 (S3 Standard-IA)
- B. 亚马逊 S3
- C. 亚马逊冰川
- D. 具有跨区域复制的 Amazon S3

答案:**B**

**Q25.** 一家公司正在 Amazon S3 上实施数据湖解决方案。其安全策略要求存储在 Amazon S3 中的数据应在静态时进行加密。

哪些选项可以实现这一目标？(选择两个。)

- A. 将 S3 服务器端加密与 Amazon EC2 密钥对一起使用。
- B. 使用带有客户提供的密钥 (SSE-C) 的 S3 服务器端加密。
- C. 使用 S3 存储桶策略来限制对静态数据的访问。
- D. 在使用加密密钥将数据提取到 Amazon S3 之前，使用客户端加密。
- E. 在传输到 Amazon S3 时，使用 SSL 加密数据。

答案:**BD** 淘宝：国际认证大师 微信：ANYPASS

**Q26.** 解决方案架构师已经创建了一个新的 AWS 账户，并且必须确保 AWS 账户 root 用户访问权限。

哪种动作组合可以达到目的？(选择两个。)

- A. 确保 root 用户使用强密码
- B. 对根用户启用多因素身份验证
- C. 将 root 用户访问密钥存储在加密的 Amazon S3 存储桶中
- D. 将 root 用户添加到包含管理权限的组中。
- E. 使用内联策略文档将所需权限应用于根用户

答案:**AB**

有几种保护根用户帐户安全的最佳实践：

锁定根用户访问密钥，或者尽可能删除它们

使用强密码

启用多因素身份验证 (MFA)

**root** 用户将自动拥有对该帐户的全部特权，并且不能限制这些特权，因此遵循有关保护 **root** 用户帐户的最佳实践建议非常重要。

正确：“确保 **root** 用户使用强密码”是正确的答案。正确：“对根用户启用多因素身份验证”是正确的答案。错误：“将根用户访问密钥存储在加密的 Amazon S3 存储桶中”是不正确的，因为最佳做法是锁定或删除根用户访问密钥。即使已加密，S3 存储桶也不适合用于存储它们。不正确：“将 **root** 用户添加到包含管理权限的组中”是不正确的，因为这不会限制访问并且是不必要的。

错误：由于无法删除根用户帐户，“删除根用户帐户”不正确。

参考文献：

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-Compliance/aws-iam/>

**Q27.** 公司的应用程序在应用程序负载平衡器（ALB）后的 Amazon EC2 实例上运行。实例在多个可用区中的 Amazon EC2 Auto Scaling 组中运行。在每月的第一天的午夜，当月末财务计算批处理执行时，应用程序变得非常慢。这导致 EC2 实例的 CPU 利用率立即达到 100% 的峰值，从而中断了应用程序。解决方案架构师应建议什么以确保应用程序能够处理工作负载并避免停机？

- A. 在 ALB 之前配置 Amazon CloudFront 分配
- B. 根据 CPU 使用率配置 EC2 自动扩展简单扩展策略
- C. 根据月度计划配置 EC2 Auto Scaling 计划的缩放策略。
- D. 配置 Amazon ElastiCache 以从 EC2 实例中删除一些工作负载

答案：**C 淘宝：国际认证大师 微信：ANYPASS**

预定缩放比例允许您设置自己的缩放时间表。在这种情况下，可以将缩放操作安排为恰好在每个月运行报表之前执行。缩放操作会根据时间和日期自动执行。这将确保有足够的 EC2 实例来满足需求，并防止应用程序变慢。正确：“根据月度计划配置 EC2 Auto Scaling 计划的缩放策略”是正确的答案。

错误：“在 ALB 之前配置 Amazon CloudFront 分配”是不正确的，因为这更适合通过缓存内容来提供对全局用户的访问。不正确：“根据 CPU 使用率配置 EC2 Auto Scaling 简单扩展策略”是不正确的，因为这将不会阻止速度降低，因为在 CPU 达到 100% 到报告的指标与其他实例之间会有延迟被发射。

错误：“配置 Amazon ElastiCache 以从 EC2 实例中删除一些工作负载”是错误的，因为 ElastiCache 是数据库缓存，它无法替换 EC2 实例的计算功能。

参考文献：

[https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule\\_time.html](https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html) 使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-自动缩放/>

**Q28.** 一家公司正在从内部部署基础架构迁移到 AWS 云。该公司的一种应用程序将文件存储在 Windows 文件服务器场中，该服务器场使用分布式文件系统复制（DFSR）来保持数据同步。解决方案架构师需要替换文件服务器场。

解决方案架构师应使用哪种服务？

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- A.Amazon EFS
- B.亚马逊 FSx
- C.亚马逊 S3
- D.AWS Storage Gateway

答案:B

适用于 Windows 的 Amazon FSx File Server 提供了完全托管的，高度可靠的文件存储，可通过行业标准的服务器消息块（SMB）协议进行访问。Amazon FSx 构建在 Windows Server 上，并提供了丰富的管理功能集，其中包括最终用户文件还原，用户配额和访问控制列表（ACL）。此外，适用于 Windows 文件服务器的 Amazon FSx 在单可用区和多可用区部署中均支持分布式文件系统复制（DFSR），如下面的功能比较表所示。

Deployment type	SSD storage	HDD storage	DFS namespaces	DFS replication	Custom DNS name	CA shares
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		Coming soon	✓*
Multi-AZ	✓	✓	✓		Coming soon	✓*

正确：“Amazon FSx”是正确的答案。

错误：“Amazon EFS”不正确，因为EFS 仅支持 Linux 系统。不正确：“Amazon S3”不正确，因为这不是 Microsoft 文件系统的合适替代品。

错误：“AWS Storage Gateway”不正确，因为此服务主要用于将本地存储连接到云存储。它由内部安装的软件设备组成，可以与 SMB 共享一起使用，但实际上将数据存储在 S3 上。它也用于迁移。但是，在这种情况下，公司需要替换文件服务器场，Amazon FSx 是此工作的最佳选择。

参考文献：

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-fsx />

Q29. 公司的网站用于向公众出售产品。该站点在应用程序负载平衡器（ALB）后面的 Auto Scaling 组中的 Amazon EC2 实例上运行。

还有一个 Amazon CloudFront 发行版，AWS WAF 被用来防御 SQL 注入攻击。

ALB 是 CloudFront 分发的来源。最近对安全日志的审查显示，需要阻止外部恶意 IP 访问该网站。解决方案架构师应该怎么做才能保护应用程序？

- A.修改 CloudFront 分发上的网络 ACL 以添加针对恶意 IP 地址的拒绝规则

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- B. 修改 AWS WAF 的配置以添加 IP 匹配条件以阻止恶意 IP 地址
- C. 修改 ALB 后面目标组中 EC2 实例的网络 ACL 以拒绝恶意 IP 地址
- D. 修改 ALB 后面目标组中 EC2 实例的安全组以拒绝恶意 IP 地址

答案:B

新版本的 AWS Web 应用程序防火墙于 2019 年 11 月发布。使用 AWS WAF classic，您可以创建“IP 匹配条件”，而使用 AWS WAF（新版本），您可以创建“IP 设置匹配语句”。注意考试的措辞。IP 匹配条件/ IP 设置匹配语句根据一组 IP 地址和地址范围检查 Web 请求来源的 IP 地址。

使用此选项可基于请求源自的 IP 地址来允许或阻止 Web 请求。

AWS WAF 支持所有 IPv4 和 IPv6 地址范围。一个 IP 集最多可以容纳 10,000 个 IP 地址或要检查的 IP 地址范围。

正确：“修改 AWS WAF 的配置以添加 IP 匹配条件以阻止恶意 IP 地址”是正确的答案。

错误：“修改 CloudFront 分发上的网络 ACL 以添加针对恶意 IP 地址的拒绝规则”是不正确的，因为 CloudFront 不在子网中，因此网络 ACL 不适用于该子网。

错误：“修改 ALB 后面目标组中的 EC2 实例的网络 ACL 以拒绝恶意 IP 地址”是错误的，因为 EC2 实例的子网中数据的源 IP 地址将是 ELB IP 地址。

错误：“在 ALB 后面的目标组中修改 EC2 实例的安全组，以拒绝恶意 IP 地址。”不正确，因为您无法使用安全组创建拒绝规则

参考文献：

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-Compliance/aws-waf-and-shield/>

Q30. 一家营销公司正在将 CSV 文件存储在 Amazon S3 存储桶中，以进行统计分析。Amazon EC2 实例上的应用程序需要权限才能有效处理存储在 S3 存储桶中的 CSV 数据。

MOST 将安全地授予 EC2 实例对 S3 存储桶的访问权限是什么？

- A. 将基于资源的策略附加到 S3 存储桶
- B. 为具有 S3 存储桶特定权限的应用程序创建 IAM 用户
- C. 将具有最小权限的 IAM 角色与 EC2 实例配置文件相关联
- D. 将 AWS 凭证直接存储在 EC2 实例上，以供该实例上的应用程序用于 API 调用

答案:C

关键字：特权权限+ IAM 角色

AWS Identity and Access Management(IAM)使您能够安全地管理对 AWS 服务和资源的访问。使用 IAM，您可以创建和管理 AWS 用户和组，并使用权限来允许和拒绝他们对 AWS 资源的访问。

IAM 是您的 AWS 账户的一项功能，无需额外付费。您只需为用户使用其他 AWS 服务付费。

Amazon EC2 的 IAM 角色

应用程序必须使用 AWS 凭证签署其 API 请求。因此，如果您是应用程序开发人员，则需要一种策略来管理在 EC2 实例上运行的应用程序的凭据。例如，您可以安全地将 AWS 凭证分发到实例，使那些实例上的应用程序可以使用您的凭证来签署请求，同时保护您的凭证免受其他用户的侵害。但是，将凭证安全地分发到每个实例，尤其是 AWS 代表您创建的凭证，例如竞价型实例或 Auto Scaling 组中的实例，具有挑战性。旋转 AWS 凭证时，您还必须能够在每个实例上更新凭证。

我们设计了 IAM 角色，以便您的应用程序可以安全地从实例发出 API 请求，而无需您管理应用程序使用的安全证书。

您可以使用 IAM 角色委派权限来发出 API 请求，而不是创建和分发您的 AWS 凭证，如下所示：

创建一个 IAM 角色。

定义哪些帐户或 AWS 服务可以担任此角色。

定义担任角色后，应用程序可以使用哪些 API 动作和资源。

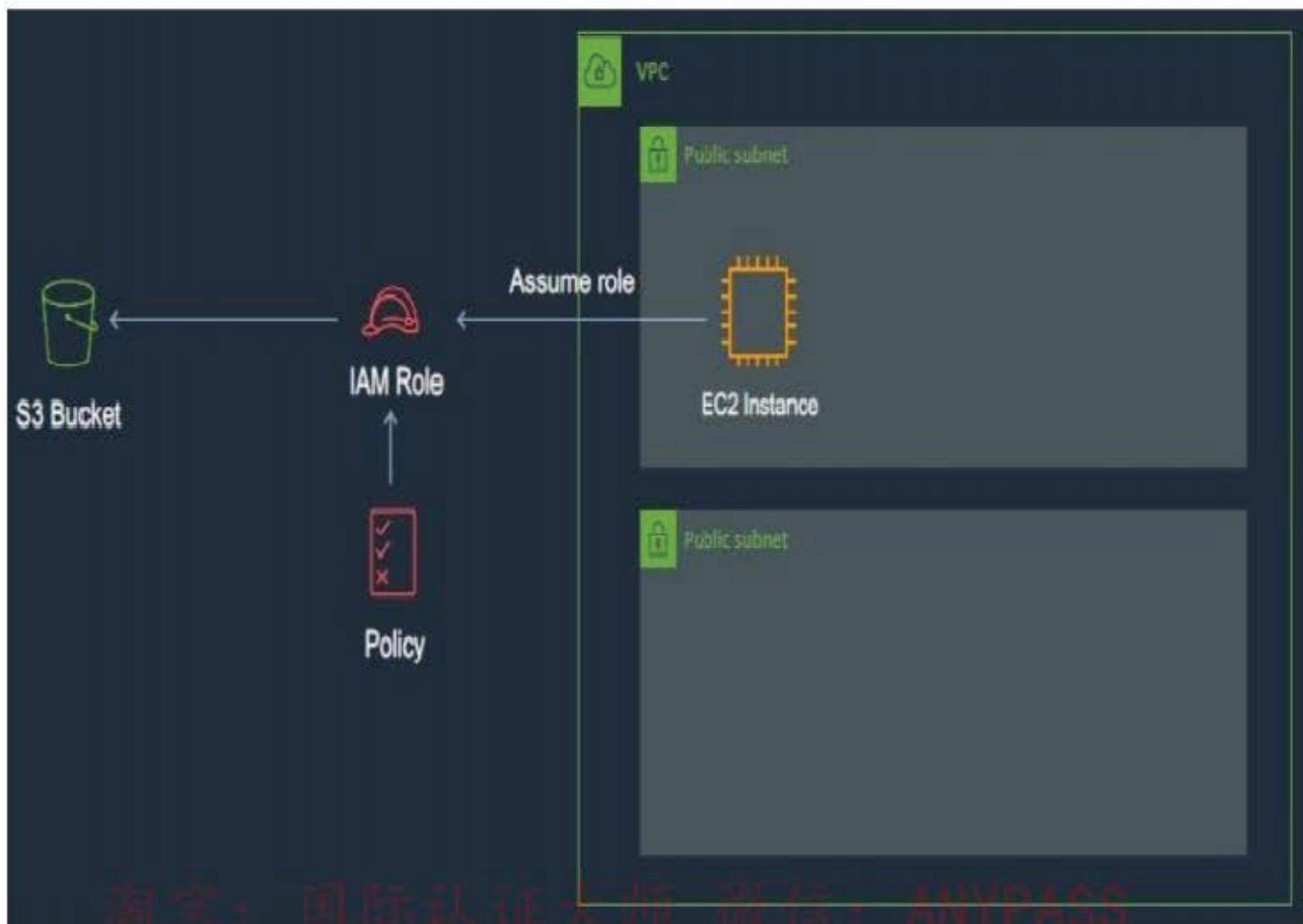
启动实例时指定角色，或将角色附加到现有实例。

让应用程序检索一组临时凭证并使用它们。

例如，您可以使用 IAM 角色向在实例上运行的需要使用 Amazon S3 中的存储桶的应用程序授予权限。您可以通过创建 JSON 格式的策略来指定 IAM 角色的权限。这些类似于您为 IAM 用户创建的策略。如果更改角色，则更改将传播到所有实例。

创建 IAM 角色时，请关联最低特权 IAM 策略，以限制对应用程序要求的特定 API 调用的访问。

IAM 角色



淘宝：国际认证大师 微信：ANYPASS



参考文献: 淘宝: 国际认证大师 微信: ANYPASS

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

<https://youtu.be/YQsK4MtsELU>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

使用我们特定于考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-Compliance/aws-iam/>

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / compute / amazon-ec2 />

**Q31.** 解决方案架构师正在设计一个解决方案，在该解决方案中，如果主网站不可用，用户将被定向到备份静态错误页面。

主网站的 DNS 记录托管在 Amazon Route 53 中，该站点的域指向应用程序负载平衡器 (ALB)。解决方案架构师应使用哪种配置来满足公司的需求，同时最大程度地减少更改和基础架构开销？

A. 将 Route 53 别名记录指向以 ALB 作为其起源之一的 Amazon CloudFront 分配。

然后，为分发创建自定义错误页面。

B. 设置 Route 53 主动-被动故障转移配置。

当 Route 53 运行状况检查确定 ALB 端点不健康时，将流量定向到 Amazon S3 存储桶中托管的静态错误页面。

C. 更新 Route 53 记录以使用基于延迟的路由策略。

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

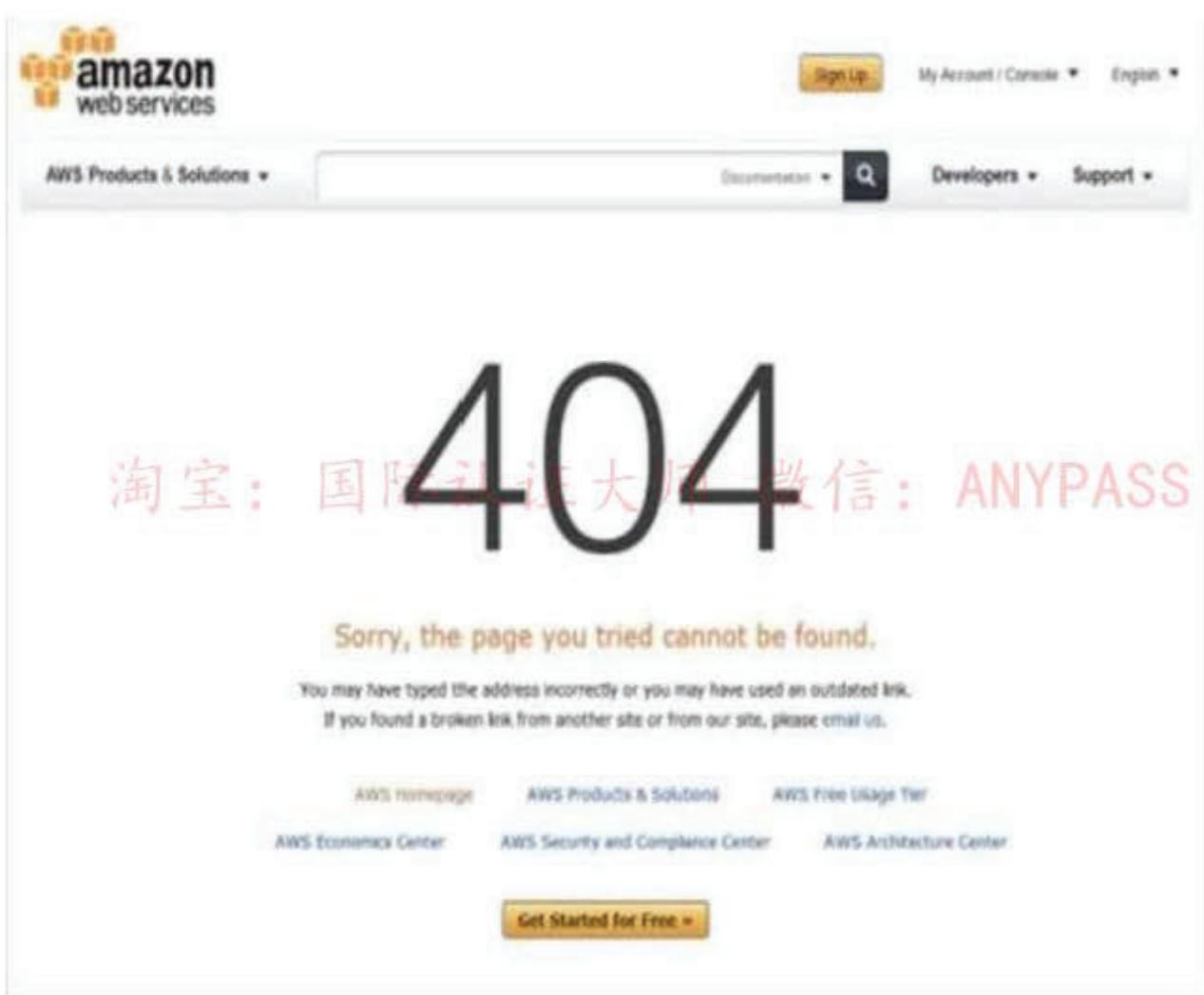
将托管在 Amazon S3 存储桶中的备份静态错误页面添加到记录中，以便将流量发送到响应速度最快的终端节点。

D. 使用 ALB 和托管静态错误页面的 Amazon EC2 实例，设置 Route 53 主动-主动配置。

如果 ALB 的运行状况检查失败，则路由 53 仅将请求发送到实例。

答案:B

将 Amazon CloudFront 用作前端可提供指定自定义消息而不是默认消息的选项。要指定您想要返回的特定文件以及应该为该文件返回的错误，您可以更新 CloudFront 发行版以指定这些值。例如，以下是自定义的错误消息：



CloudFront 发行版可以使用 ALB 作为来源，这将导致网站内容被缓存在 CloudFront 边缘缓存中。此解决方案代表了最有效的操作选择，因为除了问题的根本原因外，在出现问题时无需采取任何措施。正确：“为 Amazon CloudFront 分配创建 Route 53 别名记录，并将 ALB 指定为来源。为分配创建自定义错误页面”是正确的答案。错误：“创建 Route 53 主动-被动故障转移配置。使用承载静态错误页面的 Amazon S3 存储桶创建静态网站。将静态网站配置为故障转移的被动记录”是错误的。该选项并不代表最低的运营开销，因为需要人工干预才能导致故障回复到主网站。错误：“创建 Route 53 加权路由策略。使用托管静态错误页面的 Amazon S3 存储桶创建静态网站。将 S3 静

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

态网站的记录配置为权重为零。发生问题时，增加权重是不正确的。此选项需要人工干预，并且在管理操作进行更改之前，该问题会有所延迟。

错误：“使用 ALB 和托管静态错误页面的 Amazon EC2 实例作为端点来设置 Route 53 主动-主动配置。Route53 仅在 ALB 的运行状况检查失败时才向该实例发送请求”。通过主动-主动配置，可以在网站和错误页面之间分配流量。

参考文献：

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/custom-error-pages.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

**Q32.** 解决方案架构师正在为正在 AWS 上部署的新应用程序设计云架构。

该过程应并行运行，同时根据要处理的作业数根据需要添加和删除应用程序节点。

处理器应用程序是无状态的。

解决方案架构师必须确保应用程序松散耦合，并且持久存储作业项。

解决方案架构师应使用哪种设计？

A. 创建一个 Amazon SNS 主题以发送需要处理的作业。

创建一个由处理器应用程序组成的 Amazon Machine Image (AMI)。

创建使用 AMI 的启动配置。

使用启动配置创建一个 Auto Scaling 组。

设置 Auto Scaling 组的缩放策略以根据 CPU 使用情况添加和删除节点

B. 创建一个 Amazon SQS 队列来保存需要处理的作业。

创建一个由处理器应用程序组成的 Amazon Machine Image (AMI)。

创建使用 AMI 的启动配置。

使用启动配置创建一个 Auto Scaling 组。

为 Auto Scaling 组设置缩放策略，以根据网络使用情况添加和删除节点

C. 创建一个 Amazon SQS 队列来保存需要处理的作业。

创建一个由处理器应用程序组成的 Amazon Machine Image (AMI)。

创建使用 AMI 的启动模板

使用启动模板创建一个 Auto Scaling 组。

设置 Auto Scaling 组的缩放策略，以根据 SQS 队列中的项目数添加和删除节点

D. 创建一个 Amazon SNS 主题以发送需要处理的作业。

创建一个由处理器应用程序组成的 Amazon Machine Image (AMI)。

创建使用 AMI 的启动模板。

使用启动模板创建一个 Auto Scaling 组。

为 Auto Scaling 组设置缩放策略，以根据发布到 SNS 主题的消息数添加和删除节点。

答案:C

在这种情况下，我们需要找到一种耐用且松散耦合的解决方案来存储作业。Amazon SQS 是此用例的理想选择，可以配置为根据队列中等待的作业数使用动态扩展。

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

要配置此缩放比例，您可以使用“每个实例的待办事项”度量标准，目标值是要维护的每个实例的可接受的待办事项。您可以如下计算这些数字：

每个实例的待办事项数量：要计算每个实例的待办事项数量，请从 `roximateNumberOfMessages` 队列属性开始，以确定 SQS 队列的长度（可从队列中检索的消息数）。用该数量除以机队的运行容量，对于 Auto Scaling 组，该容量是处于 `InService` 状态的实例数，以获取每个实例的积压。

每个实例的可接受积压：要计算目标值，请首先确定您的应用程序可以接受的延迟时间。然后，将可接受的等待时间值除以 EC2 实例处理消息所需的平均时间。该解决方案将根据 SQS 队列中等待的作业数量，使用 Auto Scaling 扩展 EC2 实例。

正确：“创建一个 Amazon SQS 队列来保存需要处理的作业。为计算应用程序创建一个 Amazon EC2 Auto Scaling 组。为该 Auto Scaling 组设置扩展策略，以根据项目数添加和删除节点在 SQS 队列中”是正确的答案。

错误：“创建一个 Amazon SQS 队列来容纳需要处理的作业。为计算应用程序创建一个 Amazon EC2 Auto Scaling 组。为 Auto Scaling 组设置扩展策略以根据网络使用情况添加和删除节点。”错误，因为扩展网络使用率与等待处理的作业数量无关。错误：“创建 Amazon SNS 主题以发送需要处理的作业。为计算应用程序创建 Amazon EC2 Auto Scaling 组。为 Auto Scaling 组设置扩展策略以根据 CPU 使用率添加和删除节点。”不正确 Amazon SNS 是一项通知服务，因此它将通知发送给订户。它确实可以持久存储数据，但不适用于此用例的 SQS。扩展 CPU 使用率不是最佳解决方案，因为它与等待处理的作业数量无关。错误：“创建一个 Amazon SNS 主题以发送需要处理的作业。为计算应用程序创建一个 Amazon EC2 Auto Scaling 组。为 Auto Scaling 组设置扩展策略，以根据消息数添加和删除节点。发布到 SNS 主题”是不正确的。Amazon SNS 是一项通知服务，因此它将通知发送给订户。它确实可以持久存储数据，但不适用于此用例的 SQS。无法扩展 SNS 中的通知数量。

参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-自动缩放/> [https://digitalcloud.training/certification-training/aws-solutions-architect- associate / application-整合/ amazon-sqs /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/)

Q33. 公司有一个遗留应用程序，该应用程序分两部分处理数据。该过程的第二部分要比第一部分花费更长的时间，因此该公司决定将应用程序重写为在 Amazon ECS 上运行的两个可独立扩展的微服务。解决方案架构师应如何集成微服务？

- A. 在微服务 1 中实施代码以将数据发送到 Amazon S3 存储桶。  
使用 S3 事件通知来调用微服务 2。  
在微服务 2 中实现代码以订阅该主题。
- B. 在微服务 1 中实施代码以将数据发布到 Amazon SNS 主题。  
在微服务 2 中实现代码以订阅该主题。
- C. 在微服务 1 中实施代码以将数据发送到 Amazon Kinesis Data Firehose。  
在微服务 2 中实现代码以从 Kinesis Data Firehose 读取。
- D. 在微服务 1 中实施代码以将数据发送到 Amazon SQS 队列。  
在微服务 2 中实现代码以处理来自队列的消息。

答案:D

这是 Amazon SQS 的一个很好的用例. 微服务必须解耦, 以便它们可以独立扩展. Amazon SQS 队列将使微服务 1 将消息添加到队列. 然后, 微服务 2 可以提取消息并进行处理. 这样可以确保, 如果前端流量激增, 消息不会由于后端进程尚未准备好处理而丢失.

正确: “在微服务 1 中实施代码以将数据发送到 Amazon SQS 队列. 在微服务 2 中实施代码以处理来自队列的消息”是正确的答案. 错误: “在微服务 1 中实施代码以将数据发送到 Amazon S3 存储桶. 使用 S3 事件通知来调用微服务 2”是不正确的, 因为消息队列比 S3 存储桶更可取.

错误: “在微服务 1 中实施将数据发布到 Amazon SNS 主题的代码. 在微服务 2 中实施代码以订阅该主题”是不正确的, 因为向主题的通知已推送到订阅者. 在这种情况下, 我们希望第二个微服务在准备就绪时提取消息 (将它们拉出).

错误: “在微服务 1 中添加代码以将数据发送到 Amazon Kinesis Data Firehose. 在微服务 2 中实现代码以从 Kinesis Data Firehose 读取”是不正确的, 因为这不是 Firehose 的工作方式. Firehose 将数据直接发送到目的地, 而不是消息队列.

参考文献:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html> 使用我们针对考试的备忘单来节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

**Q34.** 一家电子商务公司的解决方案架构师希望将应用程序日志数据备份到 Amazon S3.

解决方案架构师不确定日志的访问频率或访问最多日志.

该公司希望通过使用适当的 S3 存储类别来尽可能降低成本. 应该实现哪种 S3 存储类别以满足这些要求?

- A. S3 冰川
- B. S3 智能分层
- C. S3 标准-不频繁访问 (S3 Standard-IA)
- D. S3 一区不频繁访问 (S3 一区-IA)

答案:B

S3 Intelligent-Tiering 存储类旨在通过自动将数据移动到最具成本效益的访问层来优化成本, 而不会影响性能或运营开销. 它通过将对象存储在两个访问层中来工作: 一个针对频繁访问而优化的层, 另一个针对不频繁访问而优化的低成本层. 这是用于智能分层的理想用例, 因为日志文件的访问模式未知. 正确: “S3 智能分层”是正确的答案. 错误: “S3 标准不频繁访问 (S3 Standard-IA)”是不正确的, 好像访问数据经常会使检索费用变得昂贵. 错误: “S3 一次区域不频繁访问 (S3 一次区域-IA)”是不正确的, 好像访问数据经常会使检索费用变得昂贵. 错误:

参考文献:

[https://aws.amazon.com/s3/storage-classes/#Unknown\\_or\\_changing\\_access](https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access) 使用我们特定于考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

**Q35.** 安全团队希望限制对团队所有 AWS 账户中特定服务或操作的访问.

所有账户均属于 AWS Organizations 中的大型组织. 该解决方案必须是可扩展的, 并且必须在单个点上可以维护权限.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

解决方案架构师应该怎么做才能做到这一点?

- A. 创建一个 ACL 以提供对服务或操作的访问.
- B. 创建一个安全组以允许帐户并将其附加到用户组
- C. 在每个帐户中创建跨帐户角色以拒绝访问服务或操作.
- D. 在根组织单位中创建服务控制策略以拒绝对服务或操作的访问

答案:D

**服务控制策略 (SCP)** 提供对组织中所有帐户的最大可用权限的集中控制, 使您可以确保帐户不超出组织的访问控制准则.



仅 SCP 不足以允许访问您组织中的帐户. 将 SCP 附加到 AWS Organizations 实体 (根, OU 或 帐户)可以定义主体可以执行哪些操作的防护栏. 您仍然需要将基于身份或基于资源的策略附加到组织帐户中的委托人或资源, 以实际向他们授予权限.

正确: “在根组织单位中创建服务控制策略以拒绝对服务或操作的访问”是正确的答案.

错误: “创建 ACL 以提供对服务或操作的访问”不正确, 因为访问控制列表未用于与 IAM 关联的权限. 权限策略与 IAM 一起使用.

错误: “创建安全组以允许帐户并将其附加到用户组”不正确, 因为**安全组是实例级防火墙** 它们不限制服务操作. 错误: “在每个帐户中创建跨帐户角色以拒绝对服务或操作的访问”是不正确的, 因为这是一个复杂的解决方案, 并且不提供集中控制.

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scp.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html)  
使用我们针对考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools / aws-organizations />

**Q36.** 您正在尝试启动 EC2 实例, 但是该实例似乎立即进入终止状态. 发生这种情况的原因可能不是什么原因?

- A. AMI 缺少必需的部分.
- B. 快照已损坏.

- C. 您需要首先在 EBS 中创建存储.
- D. 您已达到音量限制.

答案:C

Amazon EC2 提供了称为实例的虚拟计算环境. 启动实例后, AWS 建议您检查其状态, 以确认其已从挂起状态变为运行状态, 即未终止状态. 以下是 Amazon EBS 支持的实例可能立即终止的一些原因:

您已达到**音量**上限.

AMI 缺少必需的部分.

快照已损坏.

参考:

[http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_InstanceStraightToTerminated.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html)

Q37. 您已设置一个 Auto Scaling 组. Auto Scaling 组的冷却时间为 7 分钟. 第一个实例在 3 分钟后启动, 而第二个实例在 4 分钟后启动. 第一个实例启动后多少分钟, Auto Scaling 会接受另一个扩展活动请求?

- A. 11 分钟
- B. 7 分钟
- C. 10 分钟
- D. 14 分钟

淘宝: 国际认证大师 微信: ANYPASS

答案:A

如果一个 Auto Scaling 组正在启动多个实例, 则**每个实例的冷却期将在该实例启动后开始**. 该组将保持锁定状态, 直到启动的最后一个实例完成其冷静期为止. 在这种情况下, 第一个实例的冷却时间在 3 分钟后开始并在第 10 分钟结束 ( $3 + 7$  冷却), 而第二个实例的冷却时间在第 4 分钟开始并在第 11 分钟 ( $4 + 7$  结束冷却). 因此, Auto Scaling 组仅会在 11 分钟后收到另一个请求.  
参考: [http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS\\_Concepts.html](http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html)

Q38. 在 Amazon EC2 容器服务组件中, 可以放置任务的容器实例的逻辑分组的名称是什么?

- A. 集群
- B. 一个容器实例
- C. 一个容器
- D. 任务定义

答案:A

Amazon ECS 包含以下组件:

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

群集是可以放置任务的容器实例的逻辑分组。容器实例是运行 Amazon ECS 代理并已注册到集群的 Amazon EC2 实例。

任务定义是对包含一个或多个容器定义的应用程序的描述。调度程序是用于在容器实例上放置任务的方法。服务是一项 Amazon ECS 服务，允许您同时运行和维护指定数量的任务定义实例。

任务是在容器实例上运行的任务定义的实例。容器是作为任务的一部分创建的 Linux 容器。参考：<http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcom.html>

**Q39.** 在 AWS 支持的情况下，为什么必须在 20 分钟内无法访问 EC2 实例，而不是允许客户立即打开票证？

- A. 因为大多数可达性问题是在不到 20 分钟的时间内通过自动化流程解决的
- B. 因为当 AWS 进行例行维护时，每天 20 分钟都无法访问所有 EC2 实例
- C. 因为所有 EC2 实例在首次启动后 20 分钟内都无法访问
- D. 由于这里列出的所有原因

答案:A

打开票证之前，EC2 实例必须在 20 分钟内无法访问，因为大多数可访问性问题都可以在不到 20 分钟的时间内由自动化流程解决，并且不需要客户采取任何措施。如果在此时间范围后仍无法访问该实例，则应在支持下打开一个案例。参考：<https://aws.amazon.com/premiumsupport/faqs/>

**Q40.** 用户能否获得有关使用 Auto Scaling 配置的每个实例开始/终止的通知？

- A. 是的，如果使用启动配置进行了配置
- B. 是的，总是
- C. 是，如果配置了 Auto Scaling 组
- D. 没有

答案:C

如果用户在创建 Auto Scaling 组时配置了通知，则可以使用 SNS 接收通知。

参考：

<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html>

**Q41.** Amazon EBS 提供了将任何 Amazon EC2 卷的备份创建到称为\_\_\_\_\_的功能。

- A. 快照
- B. 图片
- C. 实例备份
- D. 镜子

答案:A

Amazon 允许您通过快照对存储在 EBS 卷中的数据进行备份，这些快照以后可用于创建新的 EBS 卷。

参考：<http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html>

**Q42.** 要在策略声明中指定资源，您可以在 Amazon EC2 中使用其 Amazon Resource Name (ARN) 吗？

- A. 可以。
- B. 不，您不能，因为 EC2 与 ARN 不相关。
- C. 不，您不能，因为您无法在 IAM 策略中指定特定的 Amazon EC2 资源。
- D. 是的，您可以但仅针对不受该操作影响的资源。

答案：A

某些 Amazon EC2 API 操作允许您在策略中包括可以由该操作创建或修改的特定资源。要在语句中指定资源，您需要使用其亚马逊资源名称 (ARN)。

参考：<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf>

**Q43.** 在向客户推荐 Amazon Redshift 作为付费数据仓库分析其数据的替代解决方案之后，客户要求您解释为什么推荐 Redshift。以下哪一项是对他的要求的合理回应？

- A. 随着数据和查询复杂性的增长，它具有大规模的高性能。
- B. 它可以防止报告和分析处理干扰 OLTP 工作负载的性能。
- C. 您没有运行自己的数据仓库以及处理设置，持久性，监视，扩展和修补的管理负担。
- D. 列出的所有答案都是对他的问题的合理回答

答案：D

Amazon Redshift 通过使用列式存储技术来提高 I/O 效率并在多个节点之间并行化查询，从而提供快速的查询性能。Redshift 使用标准的 PostgreSQL JDBC 和 ODBC 驱动程序，从而使您可以使用各种熟悉的 SQL 客户端。数据加载速度与集群大小呈线性关系，并与 Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis 或任何启用 SSH 的主机集成。AWS 向有多种需求的客户推荐 Amazon Redshift，例如：

随着数据和查询复杂性的提高，大规模实现高性能希望防止报告和分析处理干扰 OLTP 工作负载的性能使用标准 SQL 和现有 BI 工具保留和查询大量结构化数据希望自己承担管理负担数据仓库并处理设置，持久性，监视，扩展和修补

参考：[https://aws.amazon.com/running\\_databases/#redshift\\_anchor](https://aws.amazon.com/running_databases/#redshift_anchor)

**Q44.** 新部署的标准之一是客户要使用 AWS Storage Gateway。但是，您不确定应该使用网关缓存的卷还是网关存储的卷，甚至不确定它们之间的区别。以下哪个陈述最能说明这些差异？

- A. 网关缓存使您可以将数据存储在 Amazon Simple Storage Service (Amazon S3) 中，并在本地保留经常访问的数据子集的副本。

网关存储使您可以将本地网关配置为在本地存储所有数据，然后将该数据的时间点快照异步备份到 Amazon S3.

B.网关缓存是免费的，而网关存储不是免费的.

C.网关缓存的速度比网关存储快 10 倍.

D.网关存储使您可以将数据存储在 Amazon Simple Storage Service (Amazon S3) 中，并在本地保留经常访问的数据子集的副本.

网关缓存使您可以将本地网关配置为在本地存储所有数据，然后将该数据的时间点快照异步备份到 Amazon S3.

答案:A

卷网关提供了由云支持的存储卷，您可以从本地应用程序服务器将其作为 Internet 小型计算机系统接口 (iSCSI) 设备安装. 网关支持以下卷配置:

网关缓存的卷？您将数据存储在 Amazon Simple Storage Service (Amazon S3) 中，并在本地保留了频繁访问的数据子集的副本. 网关缓存的卷可在主存储上节省大量成本，并最大限度地减少在内部扩展存储的需求. 您还保留对经常访问的数据的低延迟访问. 网关存储的卷？如果需要低延迟访问整个数据集，则可以将本地网关配置为在本地存储所有数据，然后将该数据的时间点快照异步备份到 Amazon S3. 此配置提供了持久且廉价的异地备份，您可以将其恢复到本地数据中心或 Amazon EC2. 例如，如果您需要替换容量来进行灾难恢复，则可以将备份恢复到 Amazon EC2. 参考：<http://docs>.

Q45. 用户正在美国东部地区启动 EC2 实例. 关于可用性区域的选择，AWS 建议使用以下哪个选项？

淘宝：国际认证大师 微信：ANYPASS

A.在启动实例时始终选择 AZ

B.始终为 HA 选择 US-East-1-a 区域

C.不要选择 AZ；而是让 AWS 选择 AZ

D.用户在启动实例时永远无法选择可用区域

答案:C

使用 EC2 启动实例时，AWS 建议不要选择可用区 (AZ). AWS 指定应接受默认可用区. 这是因为它使 AWS 可以根据系统运行状况和可用容量选择最佳的可用区. 如果用户启动其他实例，则仅应指定一个可用区. 这是为了指定与正在运行的实例相同或不同的可用区. 参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zone.html>

Q46. 公司的网站在 Application Load Balancer (ALB) 后面的 Amazon EC2 实例上运行.

该网站混合了动态和静态内容，全球各地的用户都在报告该网站运行缓慢.

哪些措施可以改善全球用户的网站性能？

A.创建一个 Amazon CloudFront 发行版并将 ALB 配置为来源.

然后更新 Amazon Route 53 记录以指向 CloudFront 发行版.

B.为 ALB 创建基于延迟的 Amazon Route 53 记录.

然后启动具有更大实例大小的新 EC2 实例，并在 ALB 中注册这些实例.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- C. 启动新版本。在靠近用户的不同区域中托管同一 Web 应用程序的 EC2 实例。然后，使用跨区域 VPC 对等向相同的 ALB 注册实例。
- D. 将网站托管在离用户最近的区域中的 Amazon S3 存储桶中，并删除 ALB 和 EC2 实例。然后更新 Amazon Route 53 记录以指向 S3 存储桶。

答案:A

**Amazon CloudFront** 是一个内容交付网络（CDN），可通过在世界各地的边缘位置缓存内容来提高网站性能。它可以提供动态和静态内容。这是提高网站性能的最佳解决方案。正确：“正确的答案是：创建一个 Amazon CloudFront 发行版并将 ALB 配置为来源。然后更新 Amazon Route 53 记录以指向 CloudFront 发行版”。错误：“为 ALB 创建基于延迟的 Amazon Route 53 记录。然后启动具有更大实例大小的新 EC2 实例并向 ALB 注册实例”是错误的。延迟路由基于客户端和 AWS 之间的延迟进行路由。答案中没有提及在另一个区域中创建新实例的问题，因此唯一的好处就是使用了更大的实例大小。对于动态站点，这会增加使实例保持同步的复杂性。

错误：“在靠近用户的不同区域中启动托管相同 Web 应用程序的新 EC2 实例。使用 AWS Transit Gateway 将客户连接到最近的区域”是不正确的，因为 Transit Gateway 是用于将本地网络和 VPC 连接到的服务。单个网关。

不正确：“将网站迁移到离用户最近的区域中的 Amazon S3 存储桶。然后创建 Amazon Route 53 地理位置记录以指向 S3 存储桶”是不正确的，因为对于 S3，您只能托管静态网站，不能托管动态网站。

参考文献：

<https://aws.amazon.com/cloudfront/dynamic-content/>

使用我们特定于考试的备忘单节省时间：

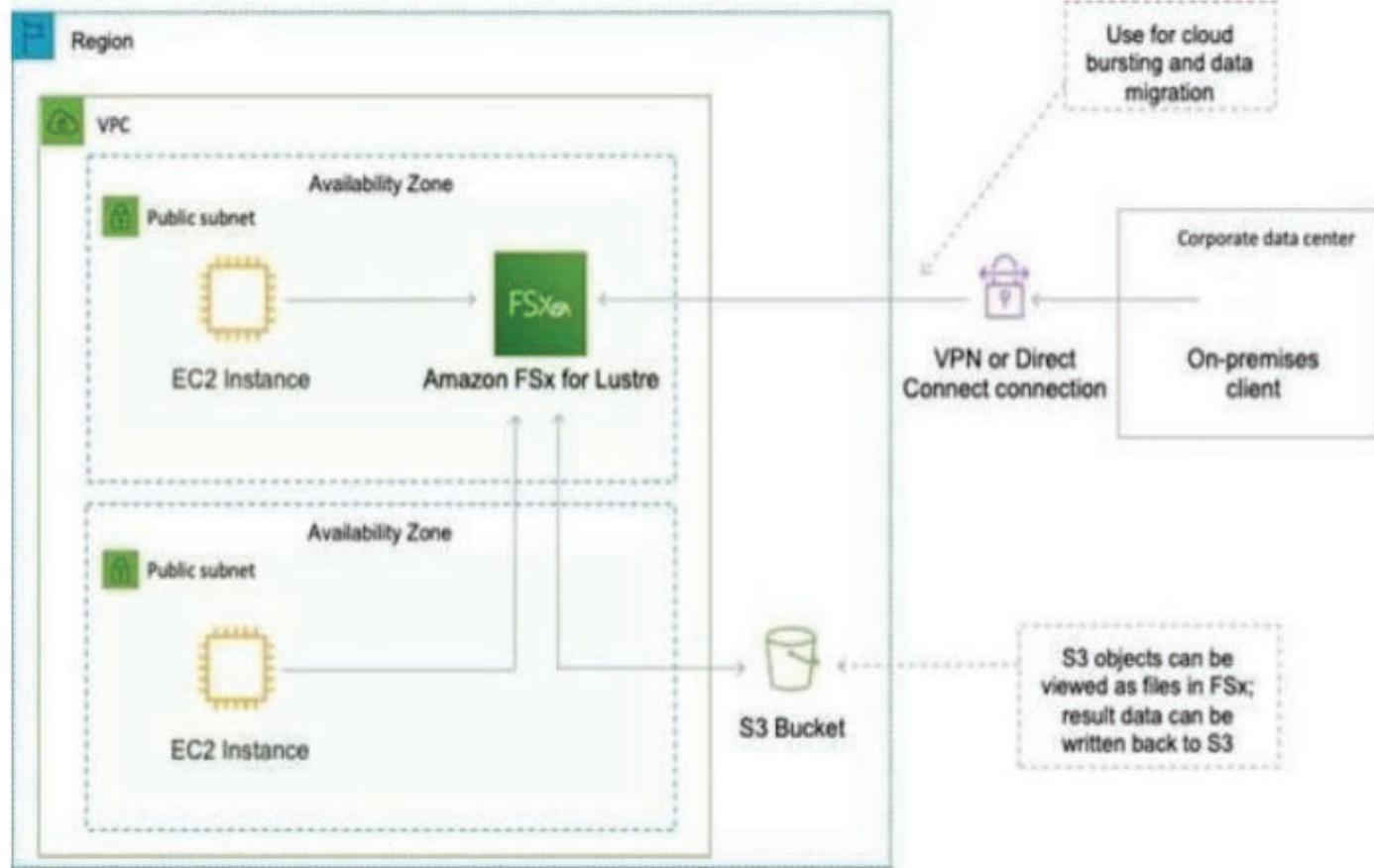
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

**Q47.** 一家公司希望将高性能计算（HPC）应用程序和数据从本地迁移到 AWS 云。该公司在本地使用分层存储，以及高性能的并行并行存储，以在应用程序的定期运行期间为应用程序提供支持，而在应用程序未主动运行时，更经济的冷存储来保存数据。解决方案架构师应建议哪种解决方案组合来支持应用程序的存储需求？（选择两个）

- A. Amazon S3 用于冷数据存储
- B. Amazon EFS 用于冷数据存储
- C. Amazon S3 用于高性能并行存储
- D. 适用于 Luster 的 Amazon FSx，用于高性能并行存储
- E. 适用于 Windows 的 Amazon FSx 用于高性能并行存储

答案:AD

**Amazon FSx for Luster** 提供了一种高性能文件系统，该文件系统经过优化，可快速处理工作负载，例如机器学习，高性能计算（HPC），视频处理，财务建模和电子设计自动化（EDA）。这些工作负载通常需要通过快速且可扩展的文件系统界面来呈现数据，并且通常将数据集存储在 Amazon S3 之类的长期数据存储中。



Amazon FSx 本机可与 Amazon S3 一起使用，从而可以轻松访问 S3 数据以运行数据处理工作负载。S3 对象在文件系统中以文件形式显示，您可以将结果写回到 S3。这使您可以在 FSx for Lustre 上运行数据处理工作负载，并将长期数据存储在 S3 或本地数据存储上。因此，此方案的最佳组合是将 S3 用于冷数据，将 FSx 用于 Lustre 用于并行 HPC 作业。

正确：“Amazon S3 用于冷数据存储”是正确的答案。正确：“适用于高性能并行存储的适用于 Lustre 的 Amazon FSx”是正确的答案。不正确：“Amazon EFS 用于冷数据存储”是不正确的，因为 FSx 可以与 S3 一起使用，这也更经济。

错误：“用于高性能并行存储的 Amazon S3”不正确，因为 S3 不适合运行高性能计算作业。错误：“适用于 Windows 的 Amazon FSx 用于高性能并行存储”是错误的，因为适用于 HPC 用例和需要在 S3 上存储数据的用例应使用适用于 Lustre 的 FSx。

参考文献：

<https://aws.amazon.com/fsx/lustre/>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-fsx />

Q48. 公司有运行关系数据库的本地服务器。当前数据库为不同位置的用户提供高读取流量。该公司希望以最少的工作量迁移到 AWS。数据库解决方案应支持灾难恢复，并且不影响公司当前的流量。

哪种解决方案满足这些要求？

- A. 在具有多可用区和至少一个只读副本的 Amazon RDS 中使用数据库

- B. 在具有多可用区和至少一个备用副本的 Amazon RDS 中使用数据库
- C. 使用托管在不同 AWS 区域中多个 Amazon EC2 实例上的数据库
- D. 在不同可用区中的应用程序负载均衡器后面使用 Amazon EC2 实例上托管的数据库

答案:A

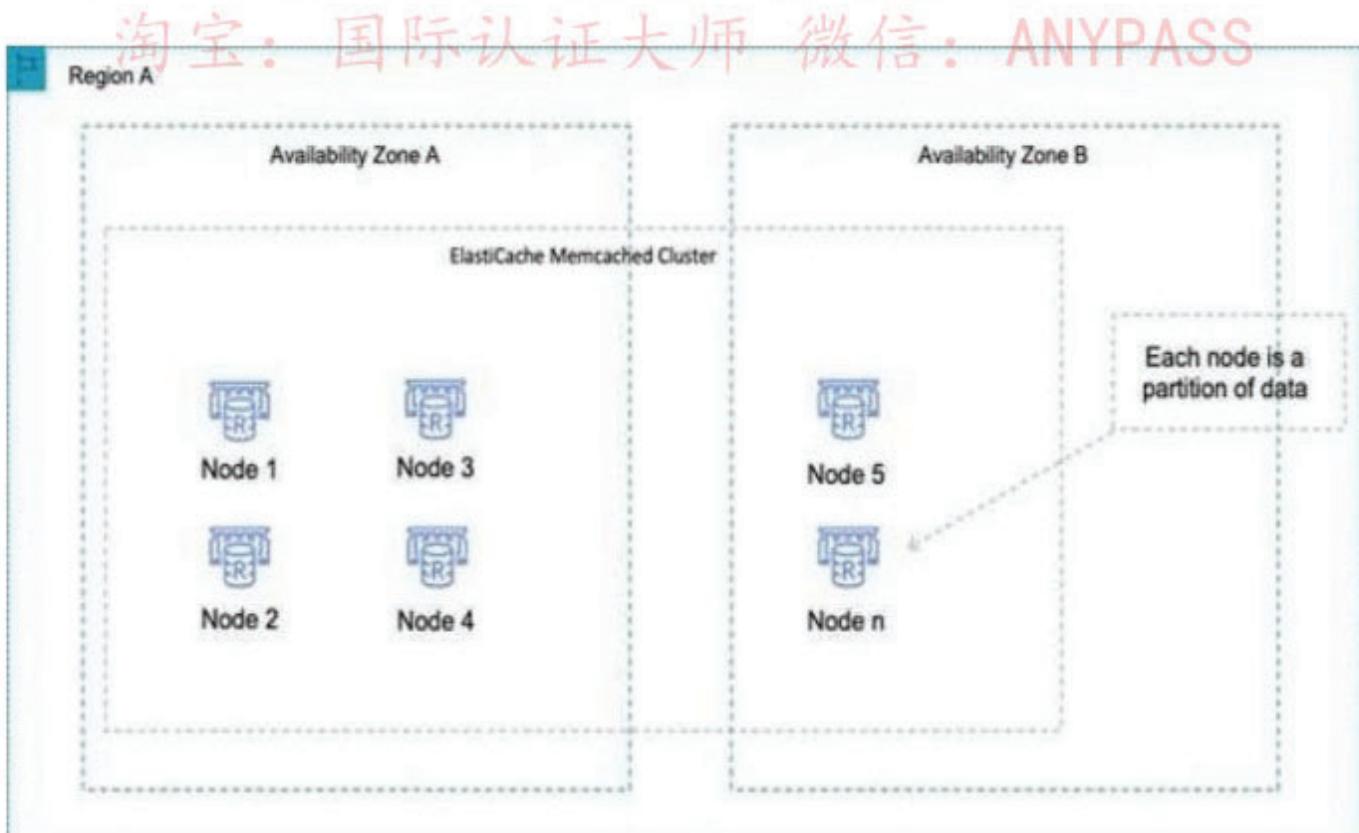
<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

**Q49.** 一家媒体流传输公司收集实时数据，并将其存储在磁盘优化的数据库系统中。该公司没有达到预期的吞吐量，而是需要一种内存中的数据库存储解决方案，该解决方案执行速度更快并使用数据复制提供高可用性。解决方案架构师应该建议哪个数据库？

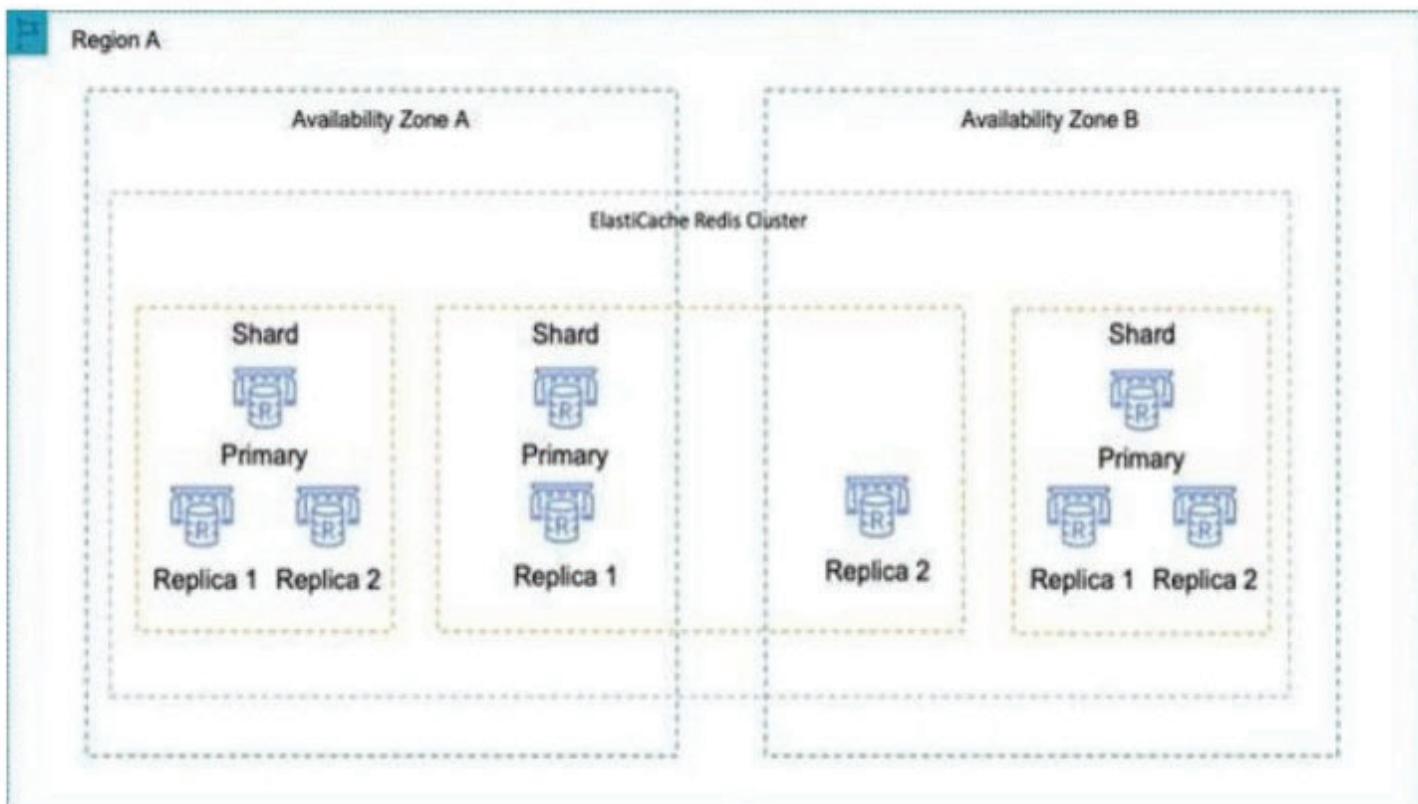
- A. 适用于 MySQL 的 Amazon RDS
- B. 适用于 PostgreSQL 的 Amazon RDS
- C. Amazon ElastiCache for Redis
- D. 用于 Memcached 的 Amazon ElastiCache

答案:C

Amazon ElastiCache 是一个内存数据库。使用 ElastiCache Memcached，不会进行数据复制或提供高可用性。如您在图中所看到的，每个节点是一个单独的数据分区：



因此，必须使用支持数据复制和群集的 Redis 引擎。下图显示了启用集群模式的 Redis 体系结构：



正确：“Amazon ElastiCache for Redis”是正确的答案。错误：“Memcached 的 Amazon ElastiCache”不正确，因为 Memcached 不支持数据复制或高可用性。

不正确：“Amazon RDS for MySQL”不正确，因为它不是内存数据库。不正确：“PostgreSQL 的 Amazon RDS”不正确，因为它不是内存数据库。

参考文献：

<https://aws.amazon.com/elasticsearch/redis/>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / database / amazon-elasticsearch />

Q50. 公司的应用程序正在 Elastic Load Balancer 后面的 Auto Scaling 组内的 Amazon EC2 实例上运行。

根据该应用程序的历史记录，该公司预计每年假期期间的流量会激增。

解决方案架构师必须设计一种策略，以确保 Auto Scaling 组能够主动增加容量，以最大程度地降低对应用程序用户的性能影响。

哪种解决方案可以满足这些要求？

- A. 创建一个 Amazon CloudWatch 警报以在 CPU 利用率超过 90% 时扩展 EC2 实例
- B. 创建一个定期计划的操作以在预期的高峰期之前扩大 Auto Scaling 组的规模
- C. 在需求高峰期增加 Auto Scaling 组中 EC2 实例的最小和最大数量
- D. 配置 Amazon Simple Notification Service (Amazon SNS) 通知以在存在自动缩放 EC2\_INSTANCE\_LAUNCH 事件时发送警报

答案:B

AWS Auto Scaling 监视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。AWS Auto Scaling 是指跨多个 AWS 服务的 Auto Scaling 功能的集合。AWS Auto Scaling 系列中的服务包括：

Amazon EC2（称为 Amazon EC2 Auto Scaling）。

Amazon ECS。

Amazon DynamoDB。

亚马逊 Aurora。

扩展选项定义触发器以及何时应提供/取消提供实例。

有四个缩放选项：

保持特定或最小数量的实例运行。

保持

使用最大、最小或特定数量的实例。

手册

淘宝：国际认证大师 微信：ANYPASS

根据计划增加或减少实例数。

预定的

根据实时系统指标（例如 CloudWatch 指标）进行扩展。

动态

下表描述了可用的缩放选项以及何时使用它们：

Scaling	What it is	When to use
Maintain	Ensures the required number of instances are running	Use when you always need a known number of instances running at all times
Manual	Manually change desired capacity via the console or CLI	Use when your needs change rarely enough that you're OK to make manual changes
Scheduled	Adjust min/max instances on specific dates/times or recurring time periods	Use when you know when your busy and quiet times are. Useful for ensuring enough instances are available <i>before</i> very busy times
Dynamic	Scale in response to system load or other triggers using metrics	Useful for changing capacity based on system utilization, e.g. CPU hits 80%

淘宝：国际认证大师 微信：ANYPASS

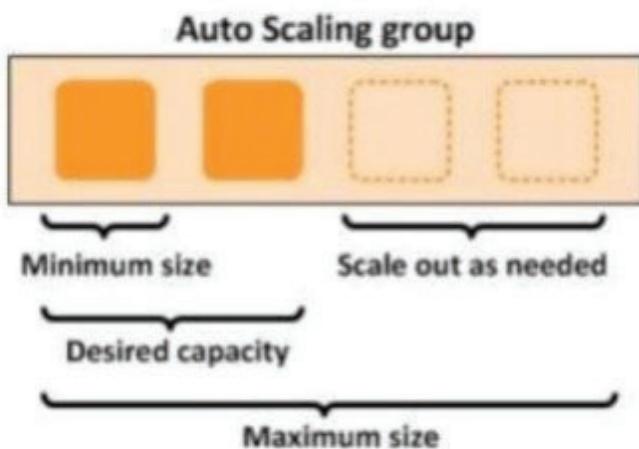
伸缩选项是通过伸缩策略配置的，伸缩策略确定 ASG 何时，是否以及如何伸缩。

下表描述了可用于动态扩展策略的扩展策略类型以及何时使用它们（在页面的下面有更多详细信息）：

Scaling Policy	What it is	When to use
Target Tracking Policy	The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value	A use case is that you want to keep the aggregate CPU usage of your ASG at 70%
Simple Scaling Policy	Waits until health check and cool down period expires before re-evaluating	This is a more conservative way to add/remove instances. Useful when load is erratic. AWS recommend step scaling instead of simple in most cases
Step Scaling Policy	Increase or decrease the current capacity of your Auto Scaling group based on a set of scaling adjustments, known as step adjustments	Useful when you want to vary adjustments based on the size of the alarm breach

淘宝：国际认证大师 微信：ANYPASS

下图描述了一个 Auto Scaling 组，其中 Scaling 策略设置为最小大小为 1 个实例，所需容量为 2 个实例，最大大小为 4 个实例：



当发生以下事件时，Amazon EC2 Auto Scaling 支持发送 Amazon SNS 通知。

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

参考文献：

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-automatic-scaling/>

[https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools-amazon-cloudwatch/)

[https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration-amazon-sns/)

**Q51.** 公司具有在公共子网和私有子网中运行的两层应用程序架构，运行 Web 应用程序的 Amazon EC2 实例位于公共子网中，而数据库在私有子网中运行。

Web 应用程序实例和数据库在单个可用区 (AZ) 中运行。解决方案架构师应采取哪些步骤组合才能为该架构提供高可用性？（选择两个。）

- A. 在同一可用区内创建新的公共和私有子网以实现高可用性
- B. 创建一个跨多个可用区的 Amazon EC2 Auto Scaling 组和 Application Load Balancer
- C. 将现有的 Web 应用程序实例添加到 Application Load Balancer 后面的 Auto Scaling 组
- D. 在新的可用区中创建新的公共和私有子网在一个可用区中使用 Amazon EC2 创建数据库
- E. 在新的可用区中的每个 VPC 中创建新的公共和私有子网，将数据库迁移到 Amazon RDS 多可用区部署

答案:BE

淘宝：国际认证大师 微信：ANYPASS

通过将 EC2 实例放置在多个可用区中，可以使它们具有高可用性。

**Q52.** 一家金融服务公司拥有一个网络应用程序，可为美国和欧洲的用户提供服务。

该应用程序由数据库层和 Web 服务器层组成。数据库层由 us-east-1 中托管的 MySQL 数据库组成。Amazon Route 53 地理邻近路由用于将流量定向到最近的 Region 中的实例。对该系统的性能检查发现，欧洲用户所获得的查询性能与美国用户不同。

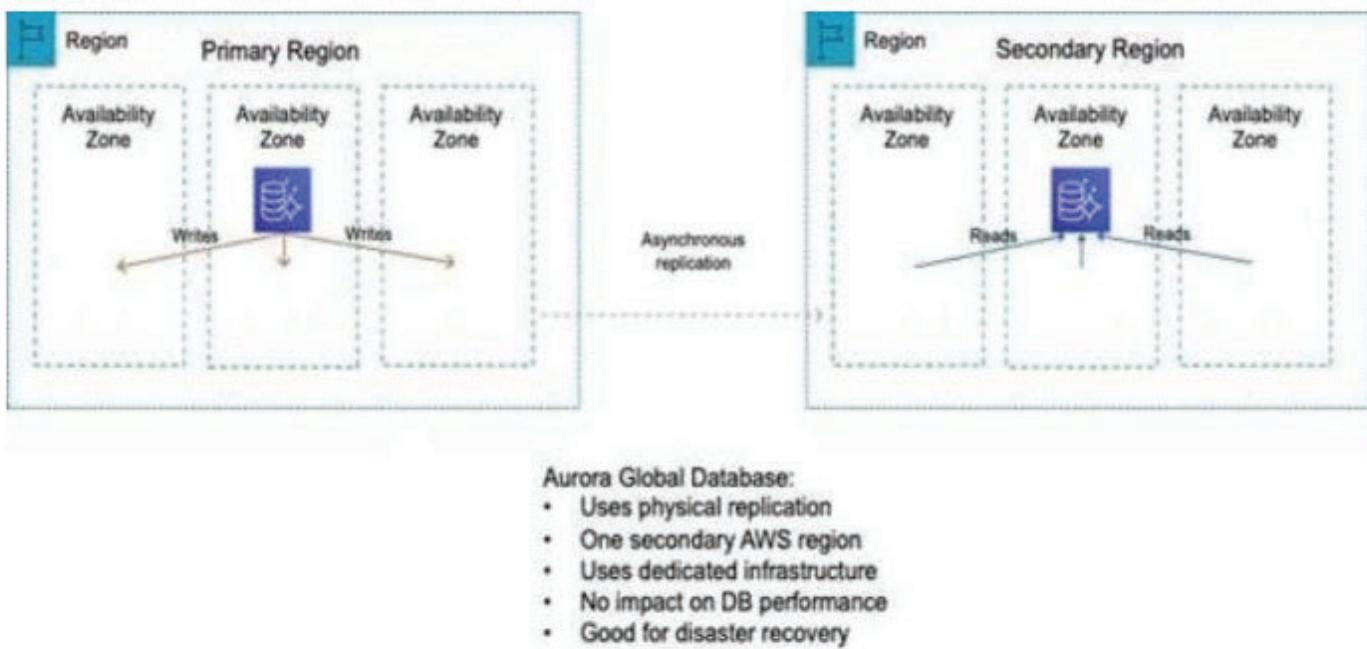
应该对数据库层进行哪些更改以提高性能？

- A. 将数据库迁移到 Amazon RDS for MySQL。  
在欧洲地区之一中配置多可用区。
- B. 将数据库迁移到 Amazon DynamoDB。  
使用 DynamoDB 全局表来启用复制到其他区域的功能。
- C. 在每个区域中部署 MySQL 实例。  
在 MySQL 前面部署应用程序负载平衡器，以减少主实例上的负载。
- D. 以 MySQL 兼容模式将数据库迁移到 Amazon Aurora 全局数据库。  
在欧洲地区之一中配置只读副本。

答案:D

这里的问题是读取查询从澳大利亚指向英国的延迟，这是很大的物理距离。需要一种解决方案来提高澳大利亚的读取性能。一个 Aurora 全局数据库由一个主要的 AWS 区域（用于管理您的数据）和最多五个只读的次要 AWS 区域组成。

Aurora 以典型的延迟不到一秒的时间将数据复制到辅助 AWS 区域。您可以直接向主要 AWS 区域中的主要数据库实例发出写入操作。



## 淘宝：国际认证大师 微信：ANYPASS

该解决方案将为澳大利亚地区的用户提供更好的查询性能。写入仍必须在英国地区进行，但读取性能将大大提高。正确：“以 MySQL 兼容模式将数据库迁移到 Amazon Aurora 全局数据库。在 ap-southeast-2 中配置只读副本”是正确的答案。错误：“将数据库迁移到 Amazon RDS for MySQL。在澳大利亚地区配置多可用区”不正确。该数据库位于英国。如果数据库迁移到澳大利亚，则会出现相反的问题。多可用区无法帮助提高跨区域的查询性能。

错误：“将数据库迁移到 Amazon DynamoDB。使用 DynamoDB 全局表来启用到其他区域的复制”是不正确的，因为在 MySQL 上运行的关系数据库不太可能与 DynamoDB 兼容。

错误：“在每个区域中部署 MySQL 实例。在 MySQL 之前部署应用程序负载平衡器以减少主实例上的负载”是不正确的，因为您只能将 ALB 放在 Web 层的前面，而不是 DB 层的前面。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / database / amazon-aurora />

Q53. 解决方案架构师的任务是将 750 TB 的数据从分支机构的网络连接文件系统传输到 Amazon S3 Glacier。解决方案必须避免饱和分支机构的低带宽 Internet 连接。

什么是最具成本效益的解决方案 1？

- A. 创建到 Amazon S3 存储桶的站点到站点 VPN 隧道，然后直接传输文件。  
创建存储桶策略以强制执行 VPC 端点。

- B. 订购 10 台 AWS Snowball 设备，然后选择一个 S3 Glacier 保管库作为目的地。  
创建存储桶策略以强制执行 VPC 端点。
- C. 将网络连接的文件系统安装到 Amazon S3 并直接复制文件。  
创建生命周期策略以将 S3 对象过渡到 Amazon S3 Glacier。
- D. 订购 10 台 AWS Snowball 设备，然后选择一个 Amazon S3 存储桶作为目的地。  
创建生命周期策略以将 S3 对象过渡到 Amazon S3 Glacier。

答案:D

由于该公司的 Internet 链接是低带宽的，直接上传到 Amazon S3（准备过渡到 Glacier）将使链接饱和。最好的替代方法是使用 AWS Snowball 设备。Snowball 边缘设备最多可容纳 75 TB 的数据因此需要 10 个设备才能迁移 750 TB 的数据。

Snowball 使用硬件设备将数据移动到 AWS 中，然后将数据复制到您选择的 Amazon S3 存储桶中。从那里，生命周期策略可以将 S3 对象过渡到 Amazon S3 Glacier。

正确：“订购 10 台 AWS Snowball 设备并选择一个 Amazon S3 存储桶作为目标。创建一个生命周期策略以将 S3 对象转换到 Amazon S3 Glacier”是正确的答案。

错误：“订购 10 台 AWS Snowball 设备并选择一个 S3 Glacier 保管库作为目标。创建存储桶策略以强制执行 VPC 端点”是错误的，因为您无法将 Glacier 保管库设置为目标，它必须是 S3 存储桶。您也不能使用存储桶策略强制执行 VPC 端点。

不正确：“创建 AWS Direct Connect 连接并将数据直接迁移到 Amazon Glacier”是不正确的，因为这不是最具成本效益的选项，并且需要花费一些时间进行设置。不正确：“使用 AWS Global Accelerator 加速上传并优化可用带宽的使用”是不正确的，因为此服务未用于加速或优化来自本地网络的数据上传。

参考文献：淘宝：国际认证大师 微信：ANYPASS

<https://docs.aws.amazon.com/snowball/latest/developer-guide/specifications.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-s3 />

Q54. 公司的生产应用程序在 Amazon RDS MySQL 数据库实例上运行在线事务处理（OLTP）事务。

该公司正在启动一种新的报告工具，该工具将访问相同的数据。报告工具必须具有高可用性，并且不会影响生产应用程序的性能

如何做到这一点？

- A. 创建生产 RDS 数据库实例的每小时快照。
- B. 创建生产 RDS 数据库实例的多可用区 RDS 只读副本。
- C. 创建生产 RDS 数据库实例的多个 RDS 只读副本。**  
将只读副本放置在 Auto Scaling 组中。
- D. 创建生产 RDS 数据库实例的单可用区 RDS 只读副本。  
从副本创建第二个单可用区 RDS 只读副本。

答案:B

您可以将只读副本创建为多可用区数据库实例. Amazon RDS 在另一个可用区中创建副本的备用数据库, 以支持该副本的故障转移. 将只读副本创建为多可用区数据库实例与源数据库是否为多可用区数据库实例无关.

正确: “创建生产 RDS 数据库实例的多可用区 RDS 只读副本”是正确的答案.

错误: “创建生产 RDS 数据库实例的单可用区 RDS 只读副本. 从副本创建第二个单可用区 RDS 只读副本”是不正确的. 只读副本主要用于水平缩放. 高可用性的最佳解决方案是使用多可用区读取副本.

错误: 由于无法使用 RDS 创建跨区域多可用区部署, 因此“创建跨区域多可用区部署并在第二个区域中创建只读副本”是不正确的. 错误: “使用 Amazon Data Lifecycle Manager 自动创建和管理快照”是不正确的, 因为使用快照不是高可用性的最佳解决方案.

参考文献:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/>

USER\_SQL.Replication.ReadReplicas.html #

USER\_SQL.Replication.ReadReplicas.MultiAZ 使用我们特定于考试的备忘单可以节省时间:

[https://digitalcloud.training/certification-training/aws-solutions-architect- associate / database / amazon-rds /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate / database / amazon-rds /)

**Q55.** 公司允许其开发人员将现有的 IAM 策略附加到现有的 IAM 角色, 以实现更快的实验和敏捷性.

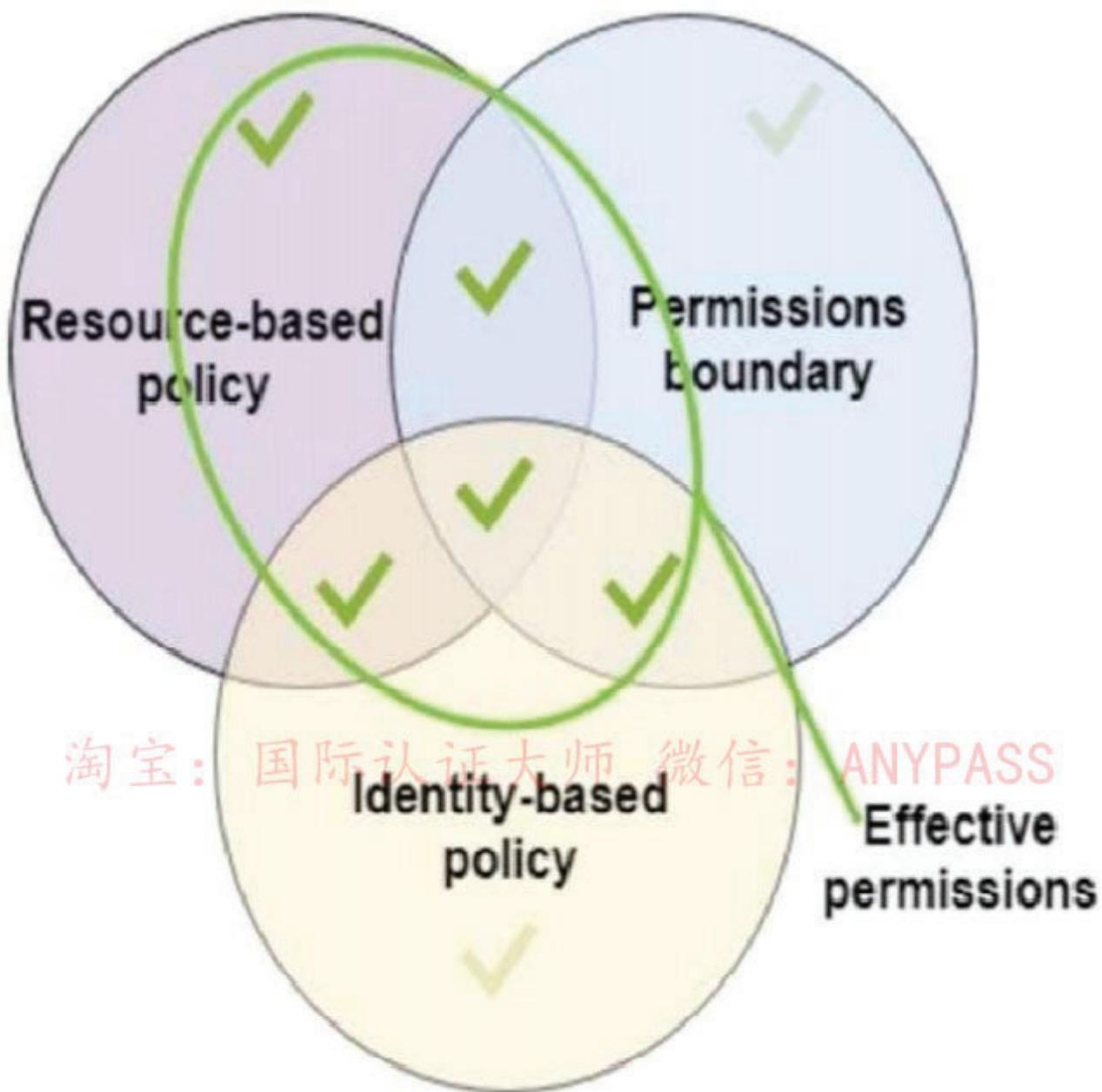
但是, 安全运营团队担心开发人员可以附加现有的管理员策略, 这将使开发人员可以规避其他任何安全策略.

解决方案架构师应如何解决此问题?

- A. 创建一个 Amazon SNS 主题, 以便在开发人员每次创建新策略时发送警报
- B. 使用服务控制策略来禁用组织单位中所有帐户的 IAM 活动
- C. 防止开发人员附加任何策略, 并将所有 IAM 职责分配给安全运营团队
- D. 在开发人员 IAM 角色上设置一个 IAM 权限边界, 该边界明确拒绝附加管理员策略

答案:D

IAM 实体(用户或角色)的权限边界设置该实体可以具有的最大权限. 这可以更改该用户或角色的有效权限. 实体的有效权限是影响用户或角色的所有策略所授予的权限. 在帐户内, 实体的权限可能会受到基于身份的策略, 基于资源的策略, 权限边界, 组织 SCP 或会话策略的影响.



因此，解决方案架构师可以在开发人员 IAM 角色上设置 IAM 权限边界，以明确拒绝附加管理员策略。正确：“在明确拒绝附加管理员策略的开发人员 IAM 角色上设置 IAM 权限边界”是正确的答案。错误：“创建一个 Amazon SNS 主题以在开发人员每次创建新策略时发送警报”是不正确的，因为这将意味着调查每个事件，而这不是一种有效的解决方案。

错误：“使用服务控制策略来禁用组织单位中所有帐户的 IAM 活动”是不正确的，因为这将阻止开发人员完全使用 IAM。

错误：“防止开发人员附加任何策略并将所有 IAM 职责分配给安全运营团队”是不正确的，因为这是不必要的。要求是允许开发人员使用策略，解决方案需要找到实现此目标的安全方法。

参考文献：

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_boundaries.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html) 使用我们针对考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-Compliance/aws-iam/>

Q56. 用户正在 AWS S3 上存储大量对象。用户希望在对象之间实现搜索功能。用户如何实现呢？

- A. 使用 S3 的索引功能。
- B. 用元数据标记对象以进行搜索。
- C. 使用 S3 的查询功能。
- D. 制作自己的数据库系统，该系统存储用于搜索功能的 S3 元数据。

答案:D

在 Amazon Web Services 中，**AWS S3 不提供任何查询工具**，要检索特定对象，用户需要知道确切的存储桶/对象键。在这种情况下，建议使用自己的数据库系统来管理 S3 元数据和键映射。参考：[http://media.amazonaws.com/AWS\\_Storage\\_Options.pdf](http://media.amazonaws.com/AWS_Storage_Options.pdf)

**Q57.** 设置了虚拟私有云（VPC）网络之后，一位经验更为丰富的云工程师建议，要实现低网络延迟和高网络吞吐量，您应该考虑设置展示位置组。您对此一无所知，但开始对其进行一些研究，并对它的局限性特别好奇。在描述展示位置组的局限性时，以下哪种说法是错误的？

- A. 尽管可以将多个实例类型启动到放置组中，但是这降低了成功启动所需容量的可能性。
- B. 放置组可以跨越多个可用区。
- C. 您不能将现有实例移动到展示位置组中。
- D. 展示位置组可以跨越对等 VPC

答案:B

放置组是单个可用区内的实例的逻辑分组。使用放置组可使应用程序参与低延迟的 10 Gbps 网络。建议**将布局组用于受益于低网络延迟，高网络吞吐量或两者兼而有之的应用程序**。要为您的展示位置组提供最低的延迟和最高的每秒数据包网络性能，请选择一个**支持增强型联网的实例类型**。展示位置组具有以下限制：

您为展示位置组指定的名称在您的 AWS 账户内必须是唯一的。展示位置组不能跨越多个可用区。尽管可以将多个实例类型启动到放置组中，但是这降低了成功启动所需容量的可能性。我们建议为展示位置组中的所有实例使用相同的实例类型。您无法合并展示位置组。相反，您必须终止一个放置组中的实例，然后将这些实例重新启动到另一个放置组中。展示位置组可以跨越对等的 VPC；但是，您不会在对等 VPC 中的实例之间获得全等带宽。有关 VPC 对等连接的更多信息，请参阅 Amazon VPC 用户指南中的 VPC 对等。**您不可以将现有实例移动到展示位置组中**。您可以从现有实例创建 AMI，然后从 AMI 启动新实例到放置组。参考：<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Q58. Amazon EC2 中的展示位置组是什么？

- A.它是单个可用区内的一组 EC2 实例.
- B.它是您的 Web 内容的边缘位置.
- C.在 AWS 区域中运行 Web 内容的 EC2 实例.
- D.这是一个用于跨越多个可用区的组.

答案:A

放置组是单个可用区内的实例的逻辑分组. 参考:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

**Q59.** 您正在将 DC 上的内部服务器迁移到具有 EBS 卷的 EC2 实例. 服务器磁盘使用量约为 500GB, 因此您仅将所有数据复制到 2TB 磁盘上即可与 AWS Import / Export 结合使用. 数据到达亚马逊后将导入哪里?

- A.到 2TB EBS 卷
- B.到带有 2 个 1TB 对象的 S3 存储桶
- C.到 500GB EBS 卷
- D.作为 2TB 快照到 S3 存储桶

答案:B

取决于存储设备的容量是小于还是等于 1 TB 还是大于 1 TB, 导入 Amazon EBS 的结果将有所不同. Amazon EBS 快照的最大大小为 1 TB, 因此, 如果设备映像大于 1 TB, 则会对映像进行分块并将其存储在 Amazon S3 上. 目标位置是根据设备的总容量而不是设备上的数据量确定的.

参考: <http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html>

**Q60.** 客户端需要您将一些现有的基础架构从专用托管提供商导入到 AWS, 以尝试并节省运行其当前网站的成本. 他还需要一个自动过程来管理备份, 软件修补, 自动故障检测和恢复. 您知道他的现有设置当前使用 Oracle 数据库. 以下哪个 AWS 数据库最适合完成此任务?

- A.Amazon RDS
- B.亚马逊 Redshift
- C.Amazon SimpleDB
- D.亚马逊 ElastiCache

答案:A

Amazon RDS 使您可以访问熟悉的 MySQL, Oracle, SQL Server 或 PostgreSQL 数据库引擎的功能. 这意味着您今天可以在现有数据库中使用的代码, 应用程序和工具可以与 Amazon RDS 一起使用. Amazon RDS 会自动修补数据库软件并备份数据库, 在用户定义的保留期内存储备份并启用时间点恢复. 参考:

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

**Q61.** 是非题: VPC 包含多个子网, 其中每个子网可以跨越多个可用区.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

- A. 只有在设置 VPC 期间提出要求时，这才是正确的。
- B. 这是真的。
- C. 这是错误的。
- D. 这仅适用于美国地区。

答案:C

一个 VPC 可以跨越多个可用区。相反，子网必须位于单个可用区中。

参考：<https://aws.amazon.com/vpc/faqs/>

#### Q62. 边缘位置是指哪个 Amazon Web Service？

- A. 边缘位置是指在区域或区域内配置的网络
- B. 边缘位置是一个 AWS 区域
- C. 边缘位置是用于 Amazon CloudFront 的数据中心的位置。
- D. 边缘位置是 AWS 区域内的区域

答案:C

Amazon CloudFront 是一个内容分发网络。内容交付网络或内容分发网络（CDN）是部署在全球多个数据中心中的大型服务器分布式系统。用于 CDN 的数据中心的位置称为边缘位置。Amazon CloudFront 可以在每个边缘位置缓存静态内容。这意味着您流行的静态内容（例如，站点的徽标，导航图像，级联样式表，JavaScript 代码等）将在附近的边缘位置可用，浏览器可以以较低的延迟下载并提高查看器的性能。

参考：<http://aws.amazon.com/cloudfront/>

#### Q63. 您正在寻找改善现有基础架构的方法，因为基本的管理和监视任务似乎占用了大量工程资源，而且成本似乎过高。您正在考虑部署 Amazon ElastiCache 来提供帮助。关于 ElastiCache，以下哪个陈述是正确的？

- A. 您可以改善对用户操作和查询的负载和响应时间，但是与扩展 Web 应用程序相关的成本会更高。
- B. 您无法改善对用户操作和查询的负载和响应时间，但可以减少与扩展 Web 应用程序相关的成本。
- C. 您可以改善对用户操作和查询的负载和响应时间，但是与扩展 Web 应用程序相关的成本将保持不变。
- D. 您可以改善对用户操作和查询的负载和响应时间，还可以减少与扩展 Web 应用程序相关的成本。

答案:D

Amazon ElastiCache 是一项 Web 服务，可轻松在云中部署和运行与 Memcached 或 Redis 协议兼容的服务器节点。Amazon ElastiCache 允许您从快速，托管的内存中缓存系统检索信息，而不是完全依赖于速度较慢的基于磁盘的数据库，从而提高了 Web 应用程序的性能。该服务简化并减轻了内存中缓存环境的管理，监视和操作，使您的工程资源可以专注于开发应用程序。使用

**Amazon ElastiCache**, 您不仅可以改善对用户操作和查询的负载和响应时间, 还可以减少与扩展 Web 应用程序相关的成本.

参考: <https://aws.amazon.com/elasticache/faqs/>

**Q64. Amazon EBS 卷是否独立于 Amazon EC2 实例的运行寿命而持久存在?**

- A.是的, 但只有在与实例分离时才这样做.
- B.不能, 您不能将 EBS 卷附加到实例.
- C.不, 他们是依赖的.
- D.是的, 他们这样做.

答案:D

**Amazon EBS 卷**的行为类似于可以附加到单个实例的原始, 未格式化的外部块设备. 该卷的持久性独立于 Amazon EC2 实例的运行寿命.

参考: <http://docs.amazonaws.com/AWSEC2/latest/UserGuide/Storage.html>

**Q65. 您的主管要求您为部门建立一个简单的文件同步服务. 他不想花太多钱, 并且希望通过电子邮件将文件更改通知给他. 您认为将哪种最佳的 Amazon 服务用于电子邮件解决方案?**

- A.亚马逊 SES
- B.亚马逊 CloudSearch
- C.亚马逊 SWF
- D.亚马逊 AppStream

答案:A

通过使用资源简单易用, 经济高效的电子邮件解决方案 **Amazon Simple Email Service (Amazon SES)** , 可以通过电子邮件将文件更改通知发送给用户.

参考:

[http://media.amazonaws.com/architecturecenter/AWS\\_ac\\_ra\\_filesync\\_08.pdf](http://media.amazonaws.com/architecturecenter/AWS_ac_ra_filesync_08.pdf)

**Q66. 产品团队正在创建一个新应用程序, 该应用程序将存储大量数据. 数据将每小时进行分析, 并由多个 Amazon EC2 Linux 实例进行修改. 应用团队认为, 在接下来的 6 个月中, 所需的空间量将继续增长.**

解决方案架构师应采取哪些行动来满足这些需求?

- A.将数据存储在 Amazon EBS 卷中.  
在应用程序实例上挂载 EBS 卷
- B.将数据存储在 Amazon EFS 文件系统中.  
在应用程序实例上挂载文件系统.
- C.将数据存储在 Amazon S3 Glacier 中.  
更新库策略以允许访问应用程序实例.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

D. 将数据存储在 Amazon S3 Standard-Infrequent Access (S3 Standard-IA) 中.  
更新存储桶策略以允许访问应用程序实例.

答案:B

Amazon Elastic File System (Amazon EFS) 提供了一个简单, 可扩展, 完全托管的弹性 NFS 文件系统, 可与 AWS Cloud 服务和本地资源一起使用. “它的构建目的是在不破坏应用程序的情况下按需扩展到 PB”, “在添加和删除文件时自动增长和收缩”, 从而无需配置和管理容量以适应增长. “数据将每小时进行分析, 并由多个 Amazon EC2 Linux 实例进行修改”

Q67. 一家游戏公司的单个多人游戏在一个可用区中具有多个 Amazon EC2 实例, 该实例与第 4 层上的用户进行通信. 首席技术官 (CTO) 希望使该架构高度可用且具有成本效益.  
解决方案架构师应该怎么做才能满足这些要求? (选择两个.)

- A. 增加 EC2 实例的数量.
- B. 减少 EC2 实例的数量
- C. 在 EC2 实例前面配置网络负载平衡器.
- D. 在 EC2 实例前面配置一个应用程序负载均衡器
- E. 配置一个 Auto Scaling 组以自动添加或删除多个可用区中的实例.

答案:CE

解决方案架构师必须为架构提供高可用性, 并确保其具有成本效益. 要启用高可用性, 应创建一个 Amazon EC2 Auto Scaling 组以跨多个可用性区域添加和删除实例. 为了将流量分发到实例, 该体系结构应使用在第 4 层运行的网络负载平衡器. 该体系结构还将具有成本效益, 因为 Auto Scaling 组将确保根据需求运行正确数量的实例. 正确: “在 EC2 实例之前配置网络负载平衡器”是正确的答案.

正确: “配置 Auto Scaling 组以自动添加或删除多个可用区中的实例”也是正确的答案.

错误: “增加实例数量并使用较小的 EC2 实例类型”是不正确的, 因为这不是最具成本效益的选择. Auto Scaling 应该用于维护正确数量的活动实例.

错误: “配置 Auto Scaling 组以自动在可用区中添加或删除实例”是不正确的, 因为它是单个 AZ, 因此不高可用性. 错误: 由于 ALB 在第 7 层而不是第 4 层运行, 因此“在 EC2 实例之前配置应用程序负载平衡器”是错误的.

参考文献:

<https://docsaws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html> 使用我们针对考试的备忘单节省时间:

[https://digitalcloud.training/certification-training/aws-solutions- architect-associate / compute / amazon-ec2 /](https://digitalcloud.training/certification-training/aws-solutions-architect- associate / compute / amazon-ec2 /) <https://digitalcloud.training/certification-training/aws-solutions- architect-associate / compute / elastic-负载均衡/>

Q68. 一家公司在多个 Amazon EC2 实例上托管一个应用程序. 该应用程序处理来自 Amazon SQS 队列写入 Amazon RDS 表的消息, 并从队列中删除该消息偶尔在 RDS 表中发现重复记录. SQS 队列不包含任何重复的消息. 归档的解决方案应该做什么以确保仅处理一次消息?

- A. 使用 CreateQueue API 调用创建一个新队列
- B. 使用 AddPermission API 调用添加适当的权限
- C. 使用 ReceiveMessage API 调用设置适当的等待时间.
- D. 使用 ChangeMessageVisibility API 调用来增加可见性超时

答案:D

关键字：SQS 队列写入 Amazon RDS

因此，选项 D 的最佳套件和其他选项被排除在外[选项 A-您不能在现有队列中再引入一个队列；选项 B-仅权限和选项 C-仅检索消息]

FIFO 队列设计为永远不会引入重复的消息。但是，您的消息生产者可能会在某些情况下引入重复项：例如，如果生产者发送了一条消息，没有收到响应，然后重新发送了同一条消息。Amazon SQS API 提供了重复数据删除功能，可防止您的消息生产者发送重复数据。消息生成者引入的所有重复项均会在 5 分钟的重复数据删除间隔内删除。

对于标准队列，您有时可能会收到消息的重复副本（至少一次传递）。如果使用标准队列，则必须将应用程序设计为幂等的（也就是说，在多次处理同一条消息时，它们不会受到不利影响）。

CreateQueue-创建队列后不能更改队列类型，也不能将现有的标准队列转换为 FIFO 队列。您必须为应用程序创建新的 FIFO 队列，或者删除现有的标准队列并将其重新创建为 FIFO 队列。

AddPermission-创建一个队列，您对该队列具有完全控制访问权限。只有您（队列的所有者）才能授予或拒绝该队列的权限。

ReceiveMessage-从指定的队列中检索一条或多条消息（最多 10 条）。

FIFO 队列提供一次精确的处理，这意味着每个消息仅传递一次并保持可用状态，直到使用者处理并删除它为止。

## Standard Queues

**Unlimited Throughput:** Standard queues support a nearly unlimited number of transactions per second (TPS) per API action.

**At-Least-Once Delivery:** A message is delivered at least once, but occasionally more than one copy of a message is delivered.

**Best-Effort Ordering:** Occasionally, messages might be delivered in an order different from which they were sent.

## FIFO Queues

**High Throughput:** By default, FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second. To request a limit increase, [file a support request](#).

**Exactly-Once Processing:** A message is delivered once and remains available until a consumer processes and deletes it. Duplicates aren't introduced into the queue.

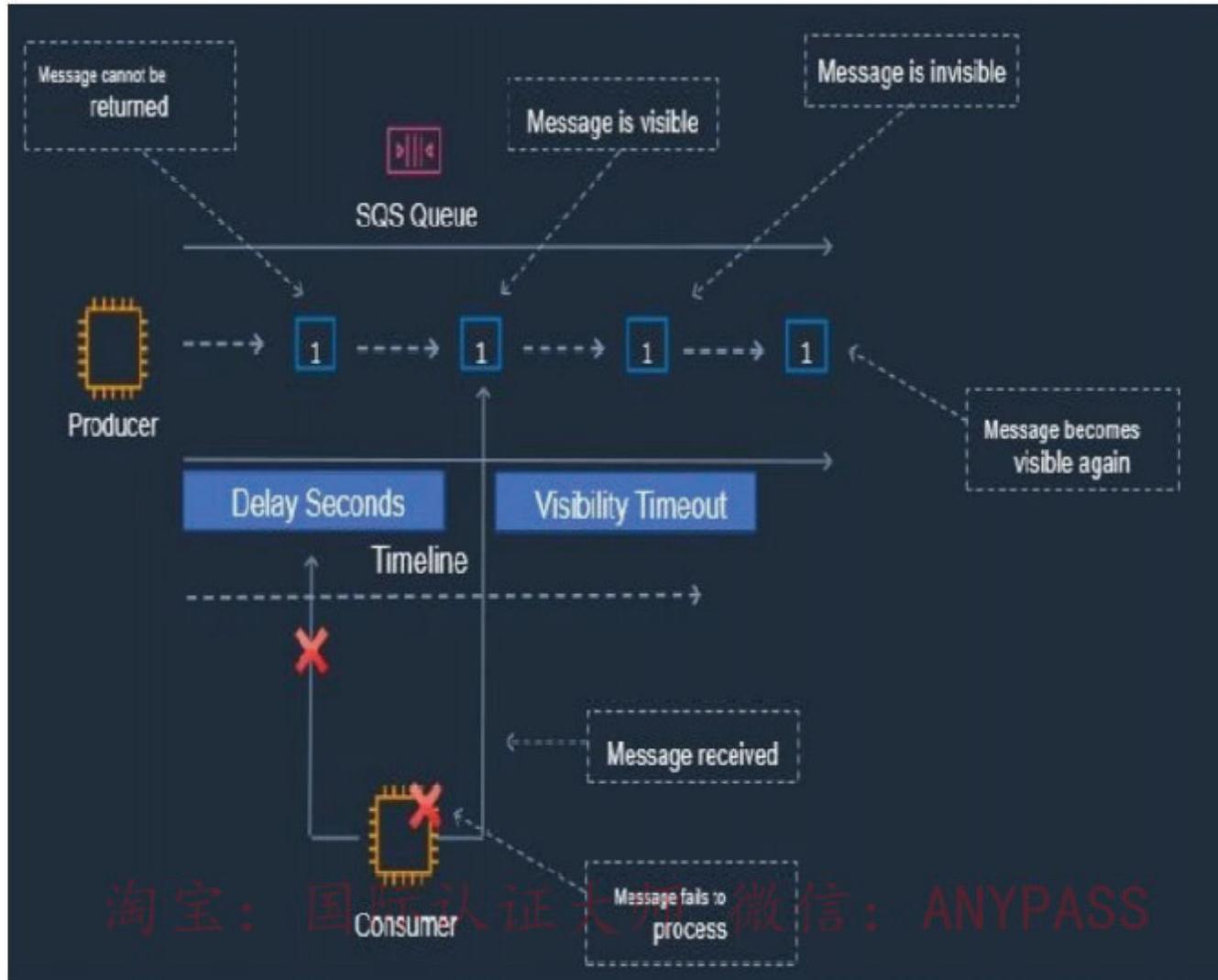
**First-In-First-Out Delivery:** The order in which messages are sent and received is strictly preserved (i.e. First-In-First-Out).



淘宝：国际认证大师 微信：ANYPASS

可见性超时  
亚马逊 SQS

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS



参考文献：

[https://aws.amazon.com/sqs/?nc2=h\\_ql\\_prod\\_ap\\_sqs](https://aws.amazon.com/sqs/?nc2=h_ql_prod_ap_sqs)

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

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html#FIFO-queues-exactly-once-processing>

<https://youtu.be/XrX7rb6M3jw>

[https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API\\_ChangeMessageVisibility.html](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_ChangeMessageVisibility.html)

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration / amazon-sqs />

**Q69.** 解决方案架构师正在为两步订购流程设计应用程序。第一步是同步的，必须以很少的延迟返回给用户。第二步需要花费更长的时间，因此将在单独的组件中实施。订单必须按接收到的顺序准确处理一次。解决方案架构师应如何集成这些组件？

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- A. 使用 Amazon SQS FIFO 队列.
- B. 将 AWS Lambda 函数与 Amazon SQS 标准队列一起使用
- C. 创建一个 SNS 主题并将 Amazon SQS FIFO 队列订阅到该主题
- D. 创建一个 SNS 主题，并将 Amazon SQS Standard 队列订阅该主题.

答案:A

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>“标准队列至少提供一次传递，这意味着每条消息至少传递一次。

FIFO 队列提供一次精确的处理，这意味着每个消息仅传递一次并保持可用状态，直到使用者处理并删除它为止。没有将重复项引入队列。”

Q70. 解决方案架构师正在 Amazon EC2 上设计高性能计算 (HPC) 工作负载.

EC2 实例需要经常相互通信，并需要低延迟和高吞吐量的网络性能.

哪种 EC2 配置符合这些要求？

- A. 在一个可用区中的群集放置组中启动 EC2 实例
- B. 在一个可用区中的扩展放置组中启动 EC2 实例
- C. 在两个区域的 Auto Scaling 组中启动 EC2 实例，并与 VPC 对等
- D. 在跨越多个可用区的 Auto Scaling 组中启动 EC2 实例

答案:A

淘宝：国际认证大师 微信：ANYPASS

当启动新的 EC2 实例时，EC2 服务将尝试以所有实例都分布在基础硬件中的方式放置该实例，以最大程度地减少相关故障。您可以使用放置组来影响一组相互依赖的实例的放置，以满足工作负载的需求。

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：

**群集**，实例在可用区中紧密靠近。该策略使工作负载能够实现 HPC 应用程序中典型的紧密耦合的节点到节点通信所需的低延迟网络性能。**分区**，将实例分散在逻辑分区中，这样一个分区中的实例组就不会与不同分区中的实例组共享基础硬件。大型分布式和复制工作负载（例如 Hadoop, Cassandra 和 Kafka）通常使用此策略。

**传播**，严格地将一小组实例放置在不同的基础硬件上，以减少相关的故障。

对于这种情况，应使用群集放置组，因为这是为 HPC 应用程序提供低延迟网络性能的最佳选择。正确：“在一个可用区中的群集放置组中启动 EC2 实例”是正确的答案。

错误：“在一个可用区中的扩展放置组中启动 EC2 实例”是不正确的，因为扩展放置组用于将实例分布在不同的基础硬件上。

错误：“在两个区域的 Auto Scaling 组中启动 EC2 实例。在实例之前放置网络负载均衡器”是不正确的，因为这不能满足在实例之间提供低延迟，高吞吐量网络性能的要求。

另外，您**不能跨区域使用 ELB**。

错误：“在跨越多个可用区的 Auto Scaling 组中启动 EC2 实例”是不正确的，因为这不会减少网络延迟或提高性能。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html> 使用我们针对考试的备忘单来节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

**Q71.** 一家公司计划使用其用户上传的 Amazon S3 存储图像。

图像必须在 Amazon S3 中静态加密。

该公司不想花费时间来管理和旋转密钥，但是它确实想控制谁可以访问这些密钥。

解决方案架构师应使用什么来完成此任务？

- A. 服务器端加密，其中密钥存储在 S3 存储桶中
- B. 使用客户提供的密钥的服务器端加密 (SSE-C)
- C. 使用 Amazon S3 托管密钥 (SSE-S3) 的服务器端加密
- D. 使用 AWS KMS 托管密钥 (SSE-KMS) 进行服务器端加密

答案:D

SSE-KMS 要求 AWS 管理数据密钥，但您需要管理 AWS KMS 中的客户主密钥 (CMK)。您可以在账户中选择客户托管的 CMK 或适用于 Amazon S3 的 AWS 托管的 CMK。

客户管理的 CMK 是您创建，拥有和管理的 AWS 账户中的 CMK。您可以完全控制这些 CMK，包括建立和维护它们的关键策略，IAM 策略和授权，启用和禁用它们，旋转其加密材料，添加标签，创建引用 CMK 的别名以及安排 CMK 进行删除。对于这种情况，解决方案架构师应将 SSE-KMS 与客户管理的 CMK 结合使用。这样，KMS 将管理数据密钥，但是公司可以配置密钥策略，定义谁可以访问密钥。

正确：“使用 AWS KMS 管理的密钥 (SSE-KMS) 进行服务器端加密”是正确的答案。

错误：“无法将密钥存储在 S3 存储桶中的服务器端加密”是不正确的，因为您无法将密钥存储在具有服务器端加密的存储桶中 错误：“使用客户提供的密钥进行服务器端加密 (SSE-C)”是错误，因为公司不想管理密钥。

错误：“使用 Amazon S3-托管密钥 (SSE-S3) 进行服务器端加密”是不正确的，因为该公司需要管理对密钥的访问控制，而这些访问控制由 Amazon 管理时是不可能的。

参考文献：

<https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse>

[https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master\\_keys](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys) 节省时间 使用我们针对考试的备忘单：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/> / <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-kms/>

Q72. Amazon EC2 管理员创建了与包含多个用户的 IAM 组关联的以下策略。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resources": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "10.100.100.0/24"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resources": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    }
  ]
}

```

淘宝店：国际认证大师 微信：ANYPASS

这项政策有什么作用？

- A. 用户可以终止除 us-east-1 之外的任何 AWS 区域中的 EC2 实例.
- B. 用户可以终止 IP 地址为 10.100 的 EC2 实例. 美国东部 1 地区的 1001.
- C. 当用户的源 IP 为 10.100.100.254 时，用户可以在 us-east-1 区域终止 EC2 实例.
- D. 当用户的源 IP 为 10.100.100.254 时，用户无法在 us-east-1 区域中终止 EC2 实例.

答案:C

Q73. 一家公司正在 Amazon EC2 上运行电子商务应用程序. 该应用程序由一个无状态 Web 层组成，该层至少需要 10 个实例，最多 250 个实例才能支持该应用程序的使用. 该应用程序需要 80% 的时间 50 个实例.

应该使用哪种解决方案以最小化成本？

- A. 购买预留实例以覆盖 250 个实例
- B. 购买预留实例以覆盖 80 个实例.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- 使用竞价型实例覆盖其余实例
- C. 购买按需实例以涵盖 40 个实例.
- 使用竞价型实例覆盖其余实例
- D. 购买预留实例以涵盖 50 个实例.
- 使用按需实例和竞价型实例覆盖其余实例

答案:D

**Q74. DynamoDB 是否支持就地原子更新?**

- A. 是的
- B. 不
- C. 它确实支持就地非原子更新
- D. 未定义

答案:A

DynamoDB 支持就地原子更新.

参考:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithItems.html#WorkingWithItems.AtomicCounters>

**Q75. 您的经理刚刚授予您访问其他人最近在公司所有办公室之间建立的多个 VPN 连接的权限. 她需要您确保 VPN 之间的通信是安全的. 以下哪项服务最适合为这些远程办公室之间的主要或备份连接提供低成本的中心辐射型模型?**

- A. Amazon CloudFront
- B. AWS 直接连接
- C. AWS CloudHSM
- D. AWS VPN CloudHub

答案:D

如果您具有多个 VPN 连接，则可以使用 AWS VPN CloudHub 在站点之间提供安全的通信. VPN CloudHub 在简单的中心辐射模型上运行，无论有无 VPC 都可以使用。此设计适用于具有多个分支机构和现有 Internet 连接的客户，这些客户希望为这些远程办公室之间的主要或备份连接实现便捷的、潜在的低成本中心辐射模型。参考：

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN\\_CloudHub.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html)

**Q76. Amazon EC2 提供了\_\_\_\_\_. 这是一个使用 HTTP 动词 GET 或 POST 的 HTTP 或 HTTPS 请求.**

- A. 网络数据库
- B. .NET 框架

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

C.查询 API  
直流图书馆

答案:C

Amazon EC2 提供了一个查询 API. 这些请求是使用 HTTP 动词 GET 或 POST 和名为 Action 的 Query 参数的 HTTP 或 HTTPS 请求. 参考:  
<http://docs.aws.amazon.com/AWSEC2/latest/APIReference/making-api-requests.html>

**Q77.** 在 Amazon AWS 中，以下哪个语句对密钥对是正确的？

- A.密钥对仅用于 Amazon SDK.
- B.密钥对仅用于 Amazon EC2 和 Amazon CloudFront.
- C.密钥对仅用于 Elastic Load Balancing 和 AWS IAM.
- D.密钥对用于所有 Amazon 服务.

答案:B

密钥对由一个公共密钥和一个私有密钥组成，您可以在其中使用私有密钥创建数字签名，然后 AWS 使用相应的公共密钥来验证签名. 密钥对仅用于 Amazon EC2 和 Amazon CloudFront.  
参考：<http://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

**Q78.** ~~淘宝店名：国际认证大师 微信： ANYPASS~~

- A.仅增量，因为 DynamoDB 的数据模型本来就不可能减小.
- B.不，既不递增也不递减操作.
- C.是的，增量和减量操作都可以.
- D.仅递减，因为 DynamoDB 的数据模型本来就不可能递增.

答案:C

Amazon DynamoDB 支持递增和递减原子操作.

参考：

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/APISummary.html>

Q79. 一个组织拥有三个单独的 AWS 账户，每个账户分别用于开发，测试和生产. 组织希望测试团队可以访问生产帐户中的某些 AWS 资源. 组织如何实现这一目标？

- A.不能使用另一个帐户访问一个帐户的资源.
- B.创建具有跨帐户访问权限的 IAM 角色.
- C.在测试帐户中创建 IAM 用户，并允许其使用 IAM 策略访问生产环境.
- D.创建具有交叉帐户访问权限的 IAM 用户.

答案:B

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信： ANYPASS

一个组织拥有多个 AWS 账户，以将开发环境与测试或生产环境隔离开。有时来自一个帐户的用户需要访问另一个帐户中的资源，例如将更新从开发环境升级到生产环境。在这种情况下，**具有交叉帐户访问权限的 IAM 角色将提供解决方案**。跨账户访问允许一个账户与另一个 AWS 账户中的用户共享对其资源的访问。

参考：[http://media.amazonwebservices.com/AWS\\_Security\\_Best\\_Practices.pdf](http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf)

**Q80.** 您需要将数百兆字节的数据从本地 Oracle 数据库导入到 Amazon RDS 数据库实例。AWS 建议您使用什么来完成此任务？

- A. Oracle 导出/导入实用程序
- B. Oracle SQL 开发人员
- C. Oracle 数据泵
- D. DBMS\_FILE\_TRANSFER

答案:C

如何将数据导入 Amazon RDS 数据库实例取决于您拥有的数据量以及数据库中数据库对象的数量和种类。例如，您可以使用 Oracle SQL Developer 导入一个简单的 20 MB 数据库。您想要使用 Oracle Data Pump 导入复杂的数据库或大小为数百兆字节或几 TB 的数据库。

参考：

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html>

**Q81.** 用户已创建具有 1000 IOPS 的 EBS 卷。如果将实例附加到 EBS 优化实例，则根据 EC2 SLA，用户一年中大部分时间的平均 IOPS 是多少？

- A. 950
- 990 年
- 约 1000
- D. 900

答案:D

根据 AWS SLA，如果将实例附加到 EBS 优化实例，则预配置 IOPS 卷的设计可在给定年份的 99.9% 的时间内交付 10% 的预配置 IOPS 性能。因此，如果用户创建了 1000 IOPS 的容量，则用户一年中至少有 99.9% 的时间获得 900 IOPS。

参考：<http://aws.amazon.com/ec2/faqs/>

**Q82.** 您需要将大量数据迁移到存储在硬盘上的云中，然后您确定实现此目标的最佳方法是使用 AWS Import / Export，然后将硬盘邮寄到 AWS。关于 AWS Import / Export，以下哪个陈述不正确？

- A. 它可以从 Amazon S3 导出

- B. 它可以导入到 Amazon Glacier
- C. 它可以从 Amazon Glacier 导出.
- D. 它可以导入到 Amazon EBS

答案:C

AWS Import / Export 支持:

- 导入到 Amazon S3
- 从 Amazon S3 导出
- 导入到 Amazon EBS
- 导入到 Amazon Glacier

AWS Import / Export 当前不支持从 Amazon EBS 或 Amazon Glacier 导出. 参考:

<https://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisdisk.html>

**Q83.** 您正在创建 Route 53 DNS 故障转移，以将流量定向到两个 EC2 区域。显然，如果其中一个发生故障，则您希望 Route 53 将流量引导到另一个区域。每个区域都有一个 ELB，其中分布有一些实例。什么是配置 Route 53 健康检查的最佳方法？

- A. Route 53 不支持带有内部运行状况检查的 ELB。您需要为 ELB 创建自己的 Route 53 运行状况检查
- B. Route 53 本机通过内部运行状况检查来支持 ELB。关闭“评估目标健康”并打开“与健康检查关联”，R53 将使用 ELB 的内部健康检查。
- C. Route 53 不支持带有内部健康检查的 ELB。您需要将 ELB 的资源记录集与您自己的健康检查相关联
- D. Route 53 本机通过内部运行状况检查支持 ELB。打开“评估目标健康”并关闭“与健康检查关联”，R53 将使用 ELB 的内部健康检查。

答案:D

通过 DNS 故障转移，Amazon Route 53 可以帮助您检测网站故障，并将最终用户重定向到您的应用程序正常运行的其他位置。启用此功能后，Route 53 会使用运行状况检查（从全球多个位置定期向应用程序的端点发出 Internet 请求）来确定应用程序的每个端点是打开还是关闭。要为 ELB 端点启用 DNS 故障转移，请创建一个指向 ELB 的别名记录，并将“评估目标运行状况”参数设置为 true。路线 53 自动为 ELB 创建和管理运行状况检查。您不需要创建自己的 ELB 的 Route 53 健康检查。您也不需要将 ELB 的资源记录集与自己的健康检查相关联，因为 Route 53 会自动将其与 Route 53 代表您管理的运行状况检查相关联。ELB 运行状况检查还将继承该 ELB 背后的后端实例的运行状况。参考：

<http://aws.amazon.com/about-aws/whats-new/2013/05/30/amazon-route-53-adds-elb-integration-for-dns-failover/>

**Q84.** 用户希望将 EBS 支持的 Amazon EC2 实例用于临时作业。根据输入的数据，该工作最有可能在一周之内完成。作业完成后，应遵循以下哪些步骤自动终止实例？

- A. 使用停止实例配置 EC2 实例以终止它。

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- B.用 ELB 配置 EC2 实例，使其在空闲时终止该实例.
- C.在实例闲置后，在应执行终止操作的实例上配置 CloudWatch 警报.
- D.配置 Auto Scaling 计划活动，该活动将在 7 天后终止实例.

答案:C

Auto Scaling 可以在预定义的时间启动和停止实例. 在这里，**总运行时间未知.** 因此，用户必须使用 CloudWatch 警报，该警报监视 CPU 利用率. 用户可以创建一个警报，该警报在 24 小时的平均 CPU 利用率百分比低于 10% 时触发，表明该警报处于空闲状态并且不再使用. 当利用率低于阈值限制时，它将作为实例操作的一部分终止实例.

参考：

<http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html>

Q85. Amazon EC2 安全组符合以下哪项要求？

- A.您可以修改 EC2-Classic 的出站规则.
- B.仅当安全组仅控制一个实例的流量时，才可以修改安全组的规则.
- C.仅当创建新实例时，才能修改安全组的规则.
- D.您可以随时修改安全组的规则.

答案:D

淘宝：国际认证大师 微信：ANYPASS

安全组充当虚拟防火墙，可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该实例相关联. 您将规则添加到每个安全组，以允许往返于其关联实例的流量. 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.

参考：

<http://docs.amazonaws.com/AWSEC2/latest/UserGuide/using-network-security.html>

Q86. 弹性 IP 地址 (EIP) 是为动态云计算设计的静态 IP 地址. 使用 EIP，您可以通过将地址快速重新映射到帐户中的另一个实例来掩盖实例或软件的故障. 您的 EIP 与您的 AWS 帐户关联，而不是与特定的 EC2 实例关联，并且在您选择明确释放它之前，它仍与您的账户关联. 默认情况下，每个 AWS 帐户每个区域限制有多少个 EIP?

- A.1
- B.5
- C.无限
- D.10

答案:B

默认情况下，每个 AWS 账户每个区域的所有 AWS 账户限制为 5 个弹性 IP 地址，因为公共 (IPv4) Internet 地址是一种稀缺的公共资源。AWS 强烈建议您 **主要将 EIP 用于负载均衡用例**，并将 DNS 主机名用于所有其他节点间通信。

如果您认为自己的架构需要其他 EIP，则需要填写 Amazon EC2 弹性 IP 地址请求表，并说明需要其他地址的原因。参考：

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-addressing-limit>

**Q87.** 在 AWS 上运行的应用程序对其数据库使用 Amazon Aurora Multi-AZ 部署。在评估性能指标时，解决方案架构师发现数据库读取导致高 I/O，并增加了对数据库的写入请求的延迟。解决方案架构师应该怎么做才能将读取请求与写入请求分开？

A. 在 Amazon Aurora 数据库上启用读缓存

**B. 更新应用程序以从多可用区备用实例读取**

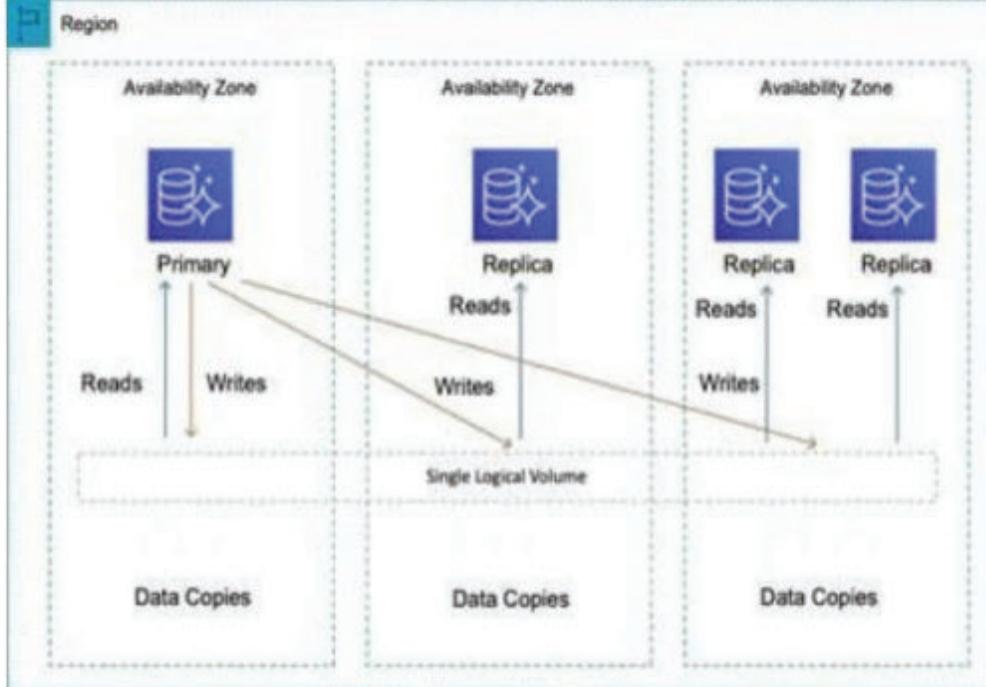
C. 创建一个只读副本并修改应用程序以使用适当的端点

D. 创建另一个 Amazon Aurora 数据库，并将其作为只读副本链接到主数据库。

答案:C

Aurora 副本是 Aurora 数据库群集中的独立端点，**最适合用于扩展读取操作和提高可用性**。最多 15 个 Aurora 副本可以分布在 AWS 区域内数据库集群所跨越的可用区中。数据库集群由数据库集群的多个数据副本组成。但是，群集卷中的数据被表示为单个实例的逻辑卷，用于主实例和数据群集中的 Aurora 副本。

淘宝：国际认证大师 微信：ANYPASS



#### Aurora Fault Tolerance

- Fault tolerance across 3 AZs
- Single logical volume
- Aurora Replicas scale-out read requests
- Up to 15 Aurora Replicas with sub-10ms replica lag
- Aurora Replicas are independent endpoints
- Can promote Aurora Replica to be a new primary or create new primary
- Set priority (tiers) on Aurora Replicas to control order of promotion
- Can use Auto Scaling to add replicas

除了提供读取缩放比例之外，Aurora 副本也是多可用区的目标。在这种情况下，解决方案架构师可以更新应用程序以从 Multi-AZ 备用实例读取。正确：“更新应用程序以从多可用区备用实例读取”是正确的答案。

错误：“创建只读副本并修改应用程序以使用适当的端点”是不正确的。Aurora 副本既是多可用区配置中的备用数据库，也是读取流量的目标。架构师只需要将流量定向到 Aurora 副本。错误：“启用对 Amazon Aurora 数据库的缓存读取。”错误，因为这不是 Amazon Aurora 的功能。

错误：“创建第二个 Amazon Aurora 数据库并将其作为只读副本链接到主数据库”不正确，因为 Aurora 副本已经存在，因为这是一个多可用区配置，而备用数据库是一个可用于读取的 Aurora 副本交通。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html> 使用我们针对考试的备忘单节省时间：

[https://digitalcloud.training/certification-training/aws-solutions-architect- associate / database / amazon-aurora /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate / database / amazon-aurora /)

**Q88.** 应用程序在多个可用区中的 Amazon EC2 实例上运行。实例在应用程序负载均衡器后面的 Amazon EC2 Auto Scaling 组中运行。当 EC2 实例的 CPU 利用率达到或接近 40% 时，该应用程序的性能最佳。解决方案架构师应如何在小组中的所有实例上保持期望的性能？

- A. 使用简单的缩放策略动态缩放 Auto Scaling 组
- B. 使用目标跟踪策略动态扩展 Auto Scaling 组
- C. 使用 AWS Lambda 函数更新所需的 Auto Scaling 组容量
- D. 使用计划的缩放操作来放大和缩小 Auto Scaling 组

答案:B 淘宝：国际认证大师 微信：ANYPASS

使用目标跟踪缩放策略，您可以选择缩放指标并设置目标值。Amazon EC2 Auto Scaling 创建和管理 CloudWatch 警报，这些警报触发扩展策略并根据指标和目标值计算扩展调整。缩放策略可根据需要添加或删除容量，以保持指标等于或接近指定目标值。除了使度量接近目标值之外，目标跟踪缩放策略还根据负载模式的变化来调整度量的变化。正确：“使用目标跟踪策略动态扩展 Auto Scaling 组”是正确的答案。

不正确：“使用简单的缩放策略来动态缩放 Auto Scaling 组”是不正确的，因为目标跟踪是一种将总 CPU 使用率保持在 40% 左右的更好方法。不正确：“使用 AWS Lambda 函数更新所需的 Auto Scaling 组容量”是不正确的，因为这可以自动完成。

错误：“使用计划的缩放操作来放大和缩小 Auto Scaling 组”是不正确的，因为需要动态缩放来响应利用率的变化。

参考文献：

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-自动缩放/>

**Q89.** 公司运行托管新闻内容的多层 Web 应用程序。该应用程序在 Application Load Balancer 后面的 Amazon EC2 实例上运行。实例在多个可用区中的 EC2 Auto Scaling 组中运行，并使用 Amazon Aurora 数据库。

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

解决方案架构师需要使应用程序更具弹性，以应对请求率的定期增加。

解决方案架构师应采用哪种架构？（选择两个）

- A.添加 AWS Shield.
- B.添加 Aurora 副本
- C.添加 AWS Direct Connect
- D.添加 AWS Global Accelerator.
- E.在 Application Load Balancer 前面添加 Amazon CloudFront 分配

答案:D E

说明

该体系结构已经具有很高的弹性，但是如果请求速率突然增加，则性能可能会下降。为了解决这种情况，Amazon Aurora 只读副本可用于提供读取流量，以减轻主数据库的请求。在前端，可以将 Amazon CloudFront 发行版放置在 ALB 的前面，这将缓存内容以获得更好的性能，还可以卸载来自后端的请求。

正确：“添加 Amazon Aurora 副本”是正确的答案。正确：“在 ALB 前面添加 Amazon CloudFront 分配”是正确的答案。

错误：“在 ALB 之前添加和 Amazon WAF”是不正确的。Web 应用程序防火墙可保护应用程序免受恶意攻击。它不会提高性能。错误：“将 Amazon Transit 网关添加到可用区”是不正确的，因为这是用于将本地网络连接到 VPC 的。

错误：“添加 Amazon Global Accelerator 终端节点”不正确，因为此服务用于根据延迟将用户定向到不同区域中的应用程序的不同实例。

参考文献：

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>  
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>  
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

Q90. 解决方案架构师正在针对即将举行的音乐活动优化网站，将实时播放表演视频，然后按需提供。该活动有望吸引全球在线观众。哪项服务将同时改善实时流和点播流的性能？

- A.Amazon CloudFront
- B.AWS 全球加速器
- C.亚马逊 53 号公路
- D.Amazon S3 传输加速

答案:A

Amazon CloudFront 可用于使用 HTTP 之上分层的多种协议向全球用户流式传输视频。这可以包括点播视频以及实时流视频。

正确：“Amazon CloudFront”是正确的答案。

不正确：“AWS Global Accelerator”不正确，因为与使用 CloudFront 相比，这是使内容更接近用户的昂贵方法。由于这是 CloudFront 的用例，并且边缘位置太多，因此是更好的选择。错误：

“Amazon Route 53”不正确，因为您仍需要一种使内容更接近用户的解决方案。

不正确：“Amazon S3 Transfer Acceleration”不正确，因为它用于加速将数据上传到 Amazon S3 存储桶。

参考文献：

<https://aws.amazon.com/cloudfront/streaming/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

**Q91.** 一家公司使用在 AWS 上运行的应用程序向其全球的订户提供内容。

该应用程序在应用程序负载平衡器（ALB）后的专用子网中具有多个 Amazon EC2 实例。

由于版权限制的最新变化，首席信息官（CIO）希望阻止某些国家/地区的访问。

哪些动作可以满足这些要求？

- A. 修改 ALB 安全组以拒绝来自阻止国家的传入流量
- B. 修改 EC2 实例的安全组以拒绝来自阻止国家的传入流量
- C. 使用 Amazon CloudFront 服务应用程序并拒绝访问被阻止的国家
- D. 使用 ALB 倾听器规则返回对来自阻止国家/地区的传入流量的拒绝访问响应

答案:C

当用户请求您的内容时，CloudFront 通常会提供请求的内容，而不管用户位于何处。如果需要阻止特定国家/地区的用户访问您的内容，则可以使用 CloudFront 地理限制功能执行以下操作之一：仅当您的用户位于已批准国家白名单中的一个国家/地区中时，才允许他们访问您的内容。

如果用户位于被禁止的国家/地区黑名单中的国家/地区之一，则可以阻止他们访问您的内容。

例如，如果请求来自出于版权原因未获授权分发内容的国家/地区，则可以使用 CloudFront 地理限制来阻止该请求。这是对内容交付实施地理限制的最简单，最有效的方法。

正确：“使用 Amazon CloudFront 服务应用程序并拒绝访问被阻止的国家”是正确的答案。

错误：“使用网络 ACL 阻止与特定国家/地区关联的 IP 地址范围”是不正确的，因为这将非常难以管理。错误：“修改 ALB 安全组以拒绝来自阻止国家的传入流量”是不正确的，因为安全组无法按国家/地区阻止流量。错误：“修改 EC2 实例的安全组以拒绝来自阻止国家的传入流量”是不正确的，因为安全组无法按国家/地区阻止流量。

参考文献：

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

Q92. 一家制造公司希望对其机械设备实施预测性维护.

该公司将安装数千个 IoT 传感器，这些传感器会实时将数据发送到 AWS. 解决方案架构师的任务是实施一种解决方案，该解决方案将按顺序接收每个机械资产的事件，并确保保存数据以供以后进行进一步处理.

哪种解决方案最有效？

A. 使用 Amazon Kinesis Data Streams 进行实时事件，并为每个设备资产分配一个分区.

使用 Amazon Kinesis Data Firehose 将数据保存到 Amazon S3.

B. 使用 Amazon Kinesis Data Streams 实时事件，并为每个设备资产分配一个碎片.

使用 Amazon Kinesis Data Firehose 将数据保存到 Amazon EBS.

C. 使用 Amazon SQS FIFO 队列处理实时事件，每个设备资产使用一个队列.

触发 SQS 队列的 AWS Lambda 函数，以将数据保存到 Amazon EFS.

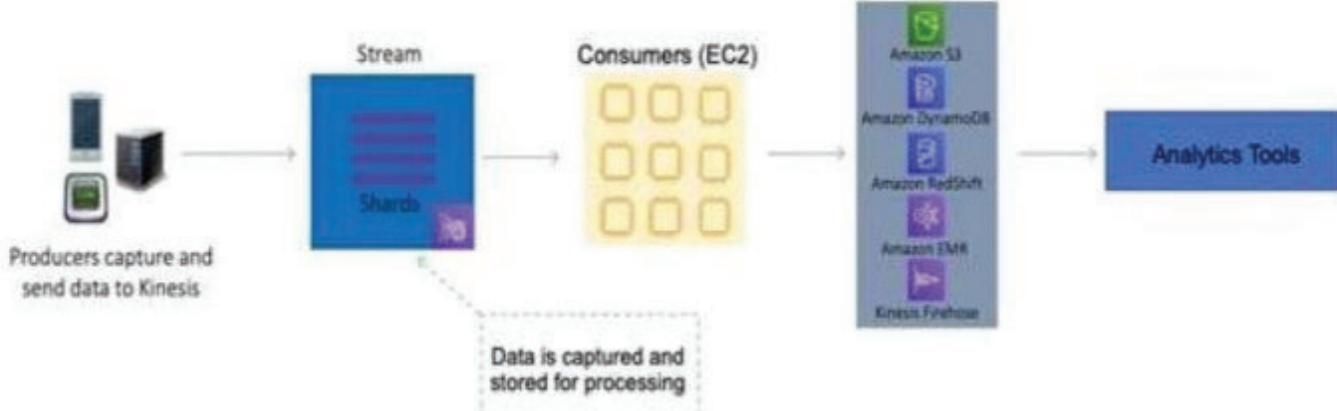
D. 使用 Amazon SQS 标准队列处理实时事件，每个设备资产使用一个队列.

从 SQS 队列触发 AWS Lambda 函数以将数据保存到 Amazon S3.

答案:A

Amazon Kinesis Data Streams 实时收集和处理数据. Kinesis 数据流是一组分片. 每个分片都有一系列数据记录. 每个数据记录都有一个序列号，该序列号由 Kinesis Data Streams 分配. **分片是流中唯一标识的数据记录序列**.

分区键用于按流中的碎片对数据进行分组. Kinesis Data Streams 将属于一个流的数据记录分成多个碎片. 它使用与每个数据记录关联的分区键来确定给定数据记录属于哪个分片.



对于这种情况，解决方案架构师可以为每个设备使用分区键. 这将确保该设备的记录按碎片分组，并且碎片将确保排序. Amazon S3 是保存数据记录的有效目的地.

正确：“将 Amazon Kinesis Data Streams 用于具有每个设备分区键的实时事件. 使用 Amazon Kinesis Data Firehose 将数据保存到 Amazon S3”是正确的答案. 错误：“将 Amazon Kinesis Data Streams 用于具有每个设备分片的实时事件. 使用 Amazon Kinesis Data Firehose 将数据保存到 Amazon EBS”是不正确的，因为您无法从 Kinesis 将数据保存到 EBS.

错误：“将 Amazon SQS FIFO 队列用于实时事件，每台设备只有一个队列。触发 SQS 队列的 AWS Lambda 函数以将数据保存到 Amazon EFS”是不正确的，因为 SQS 并不是最高效的流服务，实时数据。错误：“将 Amazon SQS 标准队列用于实时事件，每台设备一个队列。从 SQS 队列触发 AWS Lambda 函数以将数据保存到 Amazon S3”是不正确的，因为 SQS 并不是最高效的流服务，实时数据。

参考文献：

<https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html> 使用我们针对考试的备忘单节省时间：

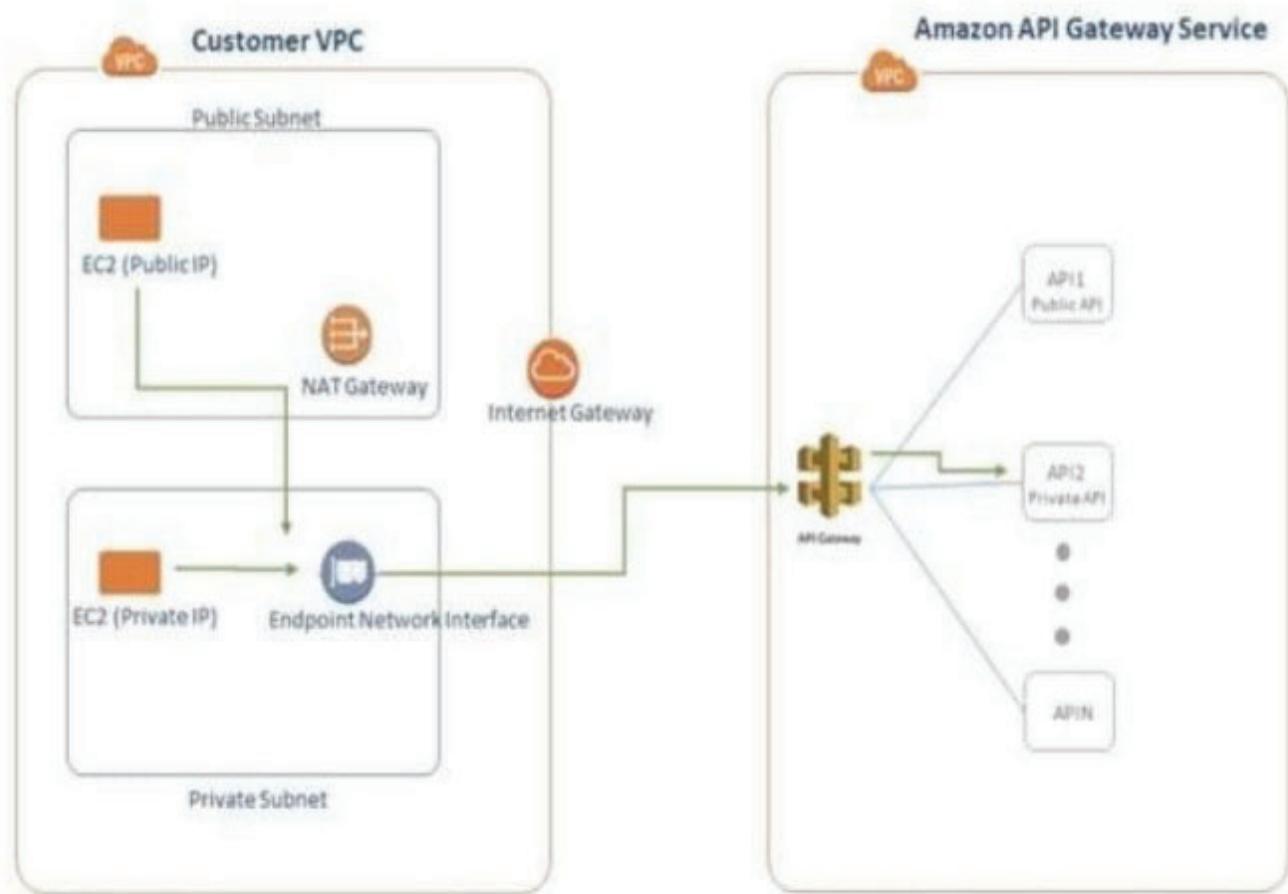
<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / analytics / amazon-kinesis />

**Q93.** 一家公司已在面向互联网的应用程序负载平衡器（ALB）后的 VPC 中部署了 API。将作为客户端使用 API 的应用程序部署在 NAT 网关后面的专用子网中的第二个帐户中。当对客户端应用程序的请求增加时，NAT 网关成本将高于预期。解决方案架构师已将 ALB 配置为内部的。哪种架构更改组合可以降低 NAT 网关的成本？（选择两个）

- A. 在两个 VPC 之间配置 VPC 对等连接。  
使用私有地址访问 API
- B. 在两个 VPC 之间配置一个 AWS Direct Connect 连接。  
使用私有地址访问 API。
- C. 为该 API 配置到客户端 VPC 的 ClassicLink 连接。  
使用 ClassicLink 地址访问 API。
- D. 配置 API 到客户端 VPC 的 PrivateLink 连接。  
使用 PrivateLink 地址访问 API。
- E. 在两个帐户之间配置一个 AWS Resource Access Manager 连接。  
使用私有地址访问 API

答案:AD

您可以在 VPC 中创建自己的应用程序，并将其配置为由 AWS PrivateLink 驱动的服务（称为终端服务）。其他 AWS 负责人可以使用接口 VPC 终端节点创建从其 VPC 到终端服务的连接。您是服务提供者，创建到服务的连接的 AWS 主体是服务使用者。



淘宝：国际认证大师 微信：ANYPASS

此配置由 AWS PrivateLink 支持，客户端无需使用 Internet 网关，NAT 设备，VPN 连接或 AWS Direct Connect 连接，也不需要公共 IP 地址。

另一种选择是使用 VPC 对等连接。VPC 对等连接是两个 VPC 之间的网络连接，使您可以使用专用 IPv4 地址或 IPv6 地址在它们之间路由通信。两个 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 之间或与另一个 AWS 账户中的 VPC 创建 VPC 对等连接。

正确：“在两个 VPC 之间配置 VPC 对等连接。使用专用地址访问 API”是正确的答案。

正确：“将 API 的 PrivateLink 连接配置到客户端 VPC。使用 PrivateLink 地址访问 API”也是正确的答案。不正确：“在两个 VPC 之间配置 AWS Direct Connect 连接。使用私有地址访问 API”是不正确的。Direct Connect 用于将内部数据中心连接到 AWS。从一个 VPC 到另一个 VPC 都不会使用它。错误：“将 API 配置到客户端 VPC 的 ClassicLink 连接。使用 ClassicLink 地址访问 API”是错误的。

**ClassicLink** 允许您将 EC2-Classic 实例链接到同一区域内您帐户中的 VPC。这与在两个 VPC 之间发送数据无关。不正确：“在两个帐户之间配置 AWS Resource Access Manager 连接。使用私有地址访问 API”是错误的。AWS RAM 使您可以共享在其他 AWS 服务中配置和管理的资源。但是，API 不能与 AWS RAM 共享资源。

参考文献：

<https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html>

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html> 使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

Q94. 在 Amazon EC2 中，部分实例小时按\_\_\_\_\_计费.

- A. 每小时使用的 A.
- B. 每分钟使用 B.
- C. 通过将部分分段合并为完整小时
- D. 全日制

答案:D

部分实例小时数将计入下一个小时.

参考: <http://aws.amazon.com/ec2/faqs/>

Q95. 在 EC2 中，如果实例（有意或无意）重新启动，实例存储中的数据将如何处理？

- A. 出于安全原因，将从实例存储中删除数据.
- B. 数据保留在实例存储中.
- C. 数据在实例存储中部分存在.
- D. 实例存储中的数据将丢失.

淘宝：国际认证大师 微信：ANYPASS

答案:B

实例存储中的数据仅在其关联实例的生存期内存在. 如果实例重新启动（有意或无意），则实例存储中的数据将保留. 但是，在以下情况下，实例存储卷上的数据会丢失.

基础驱动器故障

停止 Amazon EBS 支持的实例

终止实例

参考:

<http://docs.amazonaws.cn/AWSEC2/latest/UserGuide/InstanceStorage.html>

Q96. 您正在设置一个 VPC，并且需要在该 VPC 内设置一个公共子网. 将此子网视为公共子网必须满足以下哪些要求？

- A. 子网的流量不会路由到 Internet 网关，但是会将其流量路由到虚拟专用网关.
- B. 子网的流量被路由到 Internet 网关.
- C. 子网的流量未路由到 Internet 网关.
- D. 这些答案都不能视为公共子网.

答案:B

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

虚拟私有云 (VPC) 是专用于您的 AWS 账户的虚拟网络。它在逻辑上与 AWS 云中的其他虚拟网络隔离。您可以将您的 AWS 资源（例如 Amazon EC2 实例）启动到 VPC 中。您可以配置 VPC：您可以选择其 IP 地址范围，创建子网以及配置路由表，网络网关和安全设置。子网是 VPC 中的 IP 地址范围。您可以将 AWS 资源启动到所选的子网中。将公共子网用于必须连接到 Internet 的资源，将私有子网用于将不连接到 Internet 的资源。如果将子网的流量路由到 Internet 网关，则该子网称为公共子网。如果子网没有到 Internet 网关的路由，则该子网称为私有子网。

参考：[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Q97. 在 EC2-Classic 中启动实例时，是否可以指定为 VPC 创建的安全组？

- A. 否，您可以在启动 VPC 实例时指定为 EC2-Classic 创建的安全组。
- B. 不
- C. 是的
- D. 否，您只能将为 EC2-Classic 创建的安全组指定为仅基于非 VPC 的实例。

答案:B

如果您使用的是 EC2-Classic，则必须使用专门为 EC2-Classic 创建的安全组。在 EC2-Classic 中启动实例时，必须在与实例相同的区域中指定安全组。在 EC2-Classic 中启动实例时，无法指定为 VPC 创建的安全组。

参考：<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#ec2-classic-security-groups>

Q98. 当使用 EC2 GET 请求作为 URL 时，\_\_\_\_\_是充当 Web 服务入口点的 URL。

- A. 代币
- B. 终点
- C. 行动
- D. 这些都不是

答案:B

端点是充当 Web 服务入口点的 URL。参考：

<http://docs.amazonaws.com/AWSEC2/latest/UserGuide/using-query-api.html>

Q99. 您被要求使用 Amazon Redshift 构建数据库仓库。您对它有所了解，包括它是一个 SQL 数据仓库解决方案，并使用了行业标准的 ODBC 和 JDBC 连接以及 PostgreSQL 驱动程序。但是，您不确定它用于数据库表的存储类型。Amazon Redshift 对数据库表使用哪种存储方式？

- A. InnoDB 表

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- B. NDB 数据存储
- C. 列式数据存储
- D. NDB 群集存储

答案:C

Amazon Redshift 通过**大规模并行处理** 列式数据存储以及非常有效的目标数据压缩编码方案的组合，实现了有效的存储和最佳的查询性能。

数据库表的**列存储是优化分析查询性能的重要因素**，因为它可以大大降低总体磁盘 I/O 需求，并减少需要从磁盘加载的数据量。

参考：

[http://docs.aws.amazon.com/redshift/latest/dg/c\\_columnar\\_storage\\_disk\\_mem\\_mgmt.html](http://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmt.html)

**Q100.** 您正在检查某些通用 (SSD) 卷和预配置 IOPS (SSD) 卷上的工作负载，并且 I/O 延迟似乎比您所需的高。您可能应该检查\_\_\_\_\_，以确保您的应用程序不会尝试驱动比您提供的更多的 IOPS.

- A. 可用的 IOPS 数量
- B. 来自存储子系统的确认
- C. 平均队列长度
- D. I/O 操作完成所需的时间

答案:C

淘宝：国际认证大师 微信：ANYPASS

在 EBS 中，工作量需求在充分利用通用 (SSD) 和预配置 IOPS (SSD) 卷中起着重要作用。为了使您的卷**交付可用的 IOPS 数量，它们需要发送足够的 I/O 请求**，对卷的需求，对它们可用的 IOPS 数量与请求的延迟（完成 I/O 操作所花费的时间）之间存在关系。延迟是 I/O 操作的真实端到端客户端时间；换句话说，当客户端发送 IO 时，需要多长时间才能从存储子系统获得 IO 读写已完成的确认。

如果您的 I/O 延迟高于您的要求，请检查平均队列长度，以确保您的应用程序不会尝试驱动比您提供的更多的 IOPS。您可以通过**保持较低的平均队列长度来保持较高的 IOPS，同时降低延迟**（这可以通过为卷配置更多的 IOPS 来实现）。

参考：<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-workload-demand.html>

**Q101.** 通过 Auto Scaling 和 EC2 Classic 启动实例时，以下哪个选项不可用？

- A. 公共知识产权
- B. 弹性 IP
- C. 私人 DNS
- D. 私有 IP

答案:B

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

Auto Scaling 支持 EC2 classic 和 EC2-VPC. 当实例作为 EC2 classic 的一部分启动时, 它将具有公共 IP 和 DNS 以及私有 IP 和 DNS.

参考:

<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html>

Q102. 您已经获得了为大型组织部署一些 AWS 基础设施的范围. 要求是您将有很多 EC2 实例, 但是当 Amazon EC2 队列的平均利用率较高时, 可能需要添加更多实例; 相反, 在 CPU 利用率较低时, 则将它们删除. 最好使用哪种 AWS 服务来完成此任务?

- A. Auto Scaling, Amazon CloudWatch 和 AWS Elastic Beanstalk
- B. 自动扩展, Amazon CloudWatch 和弹性负载平衡.
- C. Amazon CloudFront, Amazon CloudWatch 和弹性负载平衡.
- D. AWS Elastic Beanstalk, Amazon CloudWatch 和 Elastic Load Balancing.

答案:B

通过 Auto Scaling, 您可以密切关注应用程序的需求曲线, 从而减少了预先手动配置 Amazon EC2 容量的需求. 例如, 您可以设置一个条件, 以在 Amazon EC2 舰队的平均利用率很高时将新的 Amazon EC2 实例以增量方式添加到 Auto Scaling 组. 同样, 您可以设置一个条件, 以在 CPU 利用率较低时以相同的增量删除实例. 如果负载变化可预测, 则可以通过 Auto Scaling 设置时间表以计划扩展活动. 您可以使用 Amazon CloudWatch 发送警报以触发扩展活动, 并可以使用 Elastic Load Balancing 帮助将流量分配到您的 Auto Scaling 组中的实例. Auto Scaling 使您能够以最佳利用率运行 Amazon EC2 机群.

参考: <http://aws.amazon.com/autoscaling/>

Q103. 公司的旧版应用程序当前依赖于未加密的单实例 Amazon RDS MySQL 数据库. 由于新的合规性要求, 必须加密此数据库中的所有现有数据和新数据. 应该如何完成?

- A. 创建一个启用了服务器端加密的 Amazon S3 存储桶.  
将所有数据移至 Amazon S3. 删除 RDS 实例.
- B. 启用 RDS 多可用区模式, 并启用静态加密.  
对备用实例执行故障转移以删除原始实例.
- C. 拍摄 RDS 实例的快照创建快照的加密副本.  
从加密的快照还原 RDS 实例.
- D. 创建一个 RDS 只读副本, 其中启用了静态加密.  
将只读副本升级为主副本, 然后将应用程序切换到新的主副本. 删除旧的 RDS 实例.

答案:C

Q104. 一家公司有一个三层的图像共享应用程序, 它在前端层使用 Amazon EC2 实例, 在后端层使用另一个实例, 而对 MySQL 数据库则使用第三个实例. 解决方案架构师的任务是设计一个高度可用的解决方案, 并且对应用程序的更改最少.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

哪种解决方案满足这些要求？

- A. 使用 Amazon S3 托管前端层，并为后端层托管 AWS Lambda 函数。  
将数据库移至 Amazon DynamoDB 表，并使用 Amazon S3 存储和提供用户图像。
- B. 将负载平衡的 Multi-AZ AWS Elastic Beanstalk 环境用于前端和后端层。  
将数据库移动到具有多个只读副本的 Amazon RDS 实例，以存储和提供用户的图像。
- C. 使用 Amazon S3 在后端的 Auto Scaling 组中托管前端层和一系列 Amazon EC2 实例。  
将数据库移至内存优化实例类型，以存储和提供用户图像。
- D. 对前端和后端层使用负载平衡的 Multi-AZ AWS Elastic Beanstalk 环境。  
将数据库移至具有多可用区部署的 Amazon RDS 实例使用 Amazon S3 存储和提供用户的图像。

答案:D

说明

关键字：高可用性+对应用程序的更改最少高可用性=多可用区

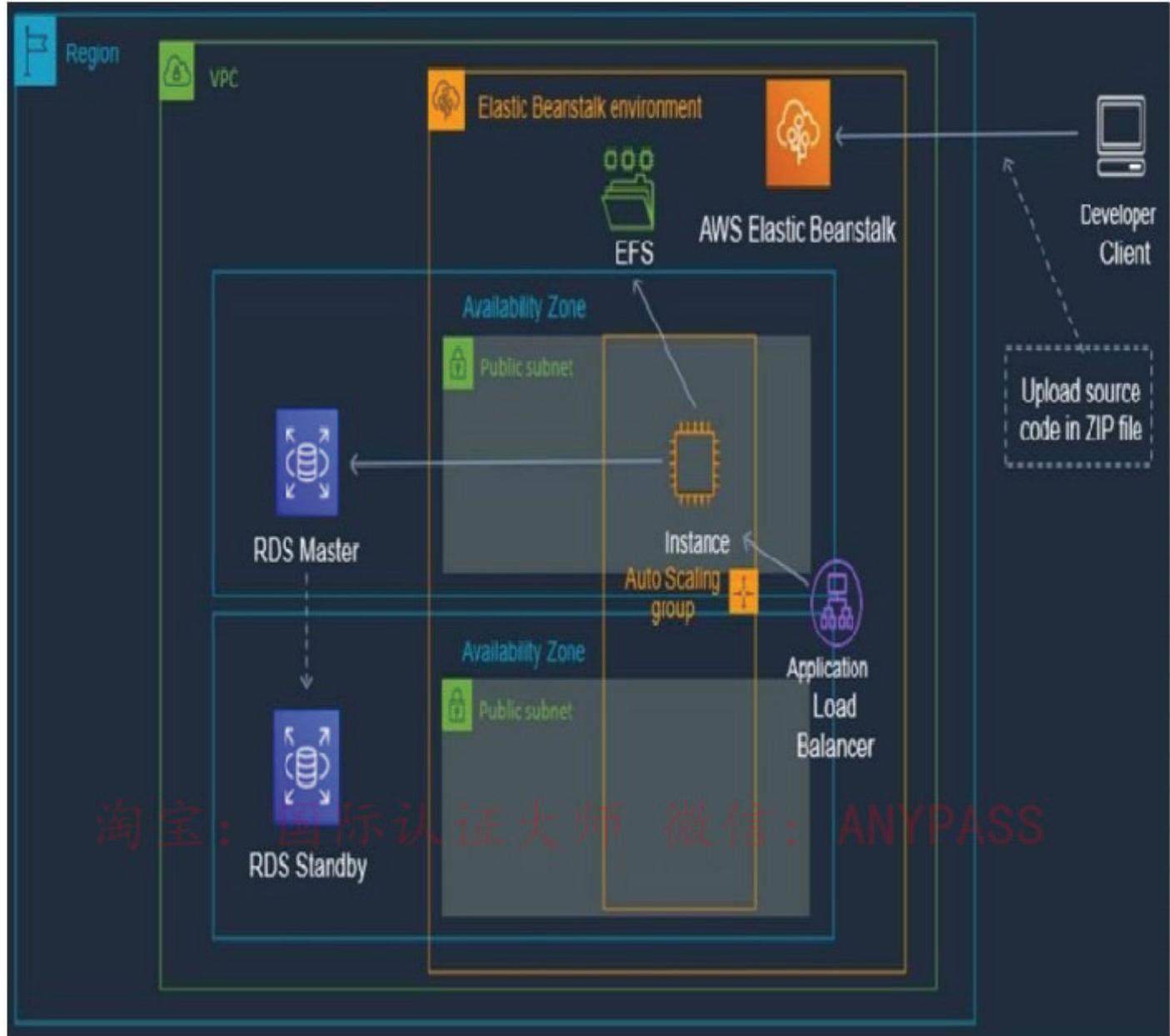
**对应用程序的最少更改= Elastic Beanstalk 自动处理**

部署，从容量配置，负载平衡，自动扩展到应用程序运行状况监视

选项-D 是正确的选择，选项-A 是正确的选择。由于成本和互操作性，选项-B 和选项-C 超出了竞争范围。

具有 Elastic Beanstalk 和 RDS 的 HA

淘宝：国际认证大师 微信：ANYPASS



## AWS Elastic Beanstalk

AWS Elastic Beanstalk 是一项易于使用的服务，用于在熟悉的服务器（例如 Apache, Nginx, Passenger）上部署和扩展使用 Java, .NET, PHP, Node.js, Python, Ruby, Go 和 Docker 开发的 Web 应用程序和服务。和 IIS。

您只需上传代码，Elastic Beanstalk 即可自动处理部署，从容量配置，负载平衡，自动扩展到应用程序运行状况监视。同时，您将完全控制为应用程序提供动力的 AWS 资源，并可以随时访问基础资源。

Elastic Beanstalk 不收取额外费用-您只需支付存储和运行应用程序所需的 AWS 资源。

## AWS RDS

Amazon Relational Database Service (Amazon RDS) 使在云中轻松设置，操作和扩展关系数据库变得容易。它提供了具有成本效益和可调整大小的容量，同时自动执行了耗时的管理任务，例如

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

硬件供应，数据库设置，修补和备份。它使您可以将精力集中在应用程序上，从而为它们提供所需的快速性能，高可用性，安全性和兼容性。

Amazon RDS 在多种数据库实例类型上可用-已针对内存，性能或 I/O 进行了优化-并为您提供了六个熟悉的数据库引擎供您选择，包括 Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database 和 SQL Server. 您可以使用 AWS 数据库迁移服务轻松地将现有数据库迁移或复制到 Amazon RDS.

### AWS S3

Amazon Simple Storage Service (Amazon S3) 是一种对象存储服务，可提供行业领先的可扩展性，数据可用性，安全性和性能。这意味着各种规模和行业的客户都可以使用它来存储和保护各种用例的任何数量的数据，例如网站，移动应用程序，备份和还原，存档，企业应用程序，IoT 设备和大数据分析. Amazon S3 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，以满足您的特定业务，组织和合规性要求. Amazon S3 专为 99.999999999% (11 9) 的耐用性而设计，并为全球范围内的公司存储着数百万个应用程序的数据。

参考文献：

[https://aws.amazon.com/elasticbeanstalk/?nc2=h\\_ql\\_prod\\_cp\\_ebs](https://aws.amazon.com/elasticbeanstalk/?nc2=h_ql_prod_cp_ebs)

[https://aws.amazon.com/rds/?nc2=h\\_ql\\_prod\\_db\\_rds](https://aws.amazon.com/rds/?nc2=h_ql_prod_db_rds)

[https://aws.amazon.com/s3/?nc2=h\\_ql\\_prod\\_st\\_s3](https://aws.amazon.com/s3/?nc2=h_ql_prod_st_s3)

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

Q105. Web 应用程序部署在 AWS Cloud 中，它由两层体系结构组成，该体系结构包含 Web 层和数据库层。

Web 服务器容易受到跨站点脚本 (XSS) 攻击。解决方案架构师应采取什么措施来补救此漏洞？

A. 创建一个经典负载均衡器。

将 Web 层放在负载均衡器后面，然后启用 AWS WAF.

B. 创建一个网络负载平衡器。

将 Web 层放在负载均衡器后面，然后启用 AWS WAF.

C. 创建一个应用程序负载平衡器。

将 Web 层放在负载均衡器后面，然后启用 AWS WAF.

D. 创建一个应用程序负载平衡器。

将 Web 层放在负载均衡器后面，然后使用 AWS Shield Standard.

答案:C

应用程序负载均衡器（ALB）上提供了 AWS Web Application Firewall（WAF）。您可以在 VPC 中的 Application Load Balancer（内部和外部）上使用 AWS WAF，以保护您的网站和 Web 服务。

攻击者有时会在 Web 请求中插入脚本，以利用 Web 应用程序中的漏洞。您可以创建一个或多个跨站点脚本匹配条件，以标识希望 AWS WAF 检查可能的恶意脚本的 Web 请求部分，例如 URI 或查询字符串。

正确：“创建应用程序负载均衡器，将 Web 层放在负载均衡器后面并启用 AWS WAF”是正确的答案。

错误：“创建经典负载均衡器，将 Web 层放在负载均衡器后面并启用 AWS WAF”是不正确的，因为您无法将 AWS WAF 与经典负载均衡器一起使用。不正确：“创建网络负载均衡器，将 Web 层置于负载均衡器后面并启用 AWS WAF”是不正确的，因为您无法将 AWS WAF 与网络负载均衡器一起使用。错误：“创建应用程序负载均衡器，将 Web 层置于负载均衡器后面并使用 AWS Shield Standard”是不正确的，因为您不能使用 AWS Shield 来防御 XSS 攻击。

**Shield 用于防御 DDoS 攻击。**

参考文献：

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-Compliance/aws-waf-and-shield/>

**Q106.** 最近需要收购的一家公司在 AWS 上构建自己的基础架构，并在一个月内将多个应用程序迁移到云中。

每个应用程序都有大约 50 TB 的数据要传输。迁移完成后，该公司及其母公司都将需要安全的网络连接，并且从其数据中心到应用程序的吞吐量始终保持一致。解决方案架构师必须确保一次性数据迁移和持续的网络连接。

哪种解决方案将满足这些要求？

- A. 适用于初始传输和持续连接的 AWS Direct Connect
- B. 适用于初始传输和持续连接的 AWS Site-to-Site VPN
- C. AWS Snowball 用于初始传输，AWS Direct Connect 用于持续连接
- D. AWS Snowball 用于初始传输，AWS Site-to-Site VPN 用于持续连接

答案：C

“每个应用程序都有大约 50 TB 的数据要传输” = AWS Snowball；“从其数据中心到应用程序的吞吐量始终保持安全的网络连接”使用 AWS Direct Connect 和专用网络连接有什么好处？在许多情况下，与基于 Internet 的连接相比，专用网络连接可以降低成本，增加带宽并提供更一致的网络体验。“更一致的网络体验”，因此是 AWS Direct Connect。

Direct Connect 比 VPN 更好：降低的成本+带宽增加+（保持连接或网络稳定）=直接连接

**Q107.** 全球活动的组织者希望将每日报告作为静态 HTML 页面放在网上。这些页面有望产生来自全球用户的数百万个视图。文件存储在 Amazon S3 存储桶中。

解决方案架构师已被要求设计一个有效的解决方案。解决方案架构师应采取什么行动来完成此任务？

- A.生成文件的预签名 URL
- B.使用跨区域复制到所有区域
- C.使用 Amazon Route 53 的 geoproximity 功能
- D.将 Amazon CloudFront 与 S3 存储桶作为源

答案:D

Amazon CloudFront 可用于在世界各地的边缘位置缓存文件，这将改善网页的性能。

要为 Amazon S3 上托管的静态网站提供服务，您可以使用以下配置之一来部署 CloudFront 分配：使用 REST API 端点作为源，并且访问受源访问身份（OAI）限制。使用网站端点作为源，并且允许匿名（公共）访问，使用网站端点作为源，访问源受到 Referer 标头的限制：

正确的答案是“将 Amazon CloudFront 与 S3 存储桶一起使用”。不正确：“生成文件的预签名 URL”不正确，因为它用于限制访问，这不是必需的。

不正确：“使用跨区域复制到所有区域”是不正确的，因为它不提供一种将用户定向到静态网页的最近副本的机制。错误：“使用 Amazon Route 53 的地理邻近性功能”是不正确的，因为它不包括在不同地理位置具有多个数据副本的解决方案。

参考文献：

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/> 通过我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

**Q108.** 一家公司在一组 Amazon Linux EC2 实例上运行一个应用程序，该应用程序使用标准 API 调用写入日志文件。出于合规性原因，所有日志文件必须无限期保留，并且将由必须同时访问所有文件的报告工具进行分析。

解决方案架构师应使用哪种存储服务来提供最具成本效益的解决方案？

- A.亚马逊 EBS
- B.亚马逊 EFS
- C.Amazon EC2 实例存储
- D.亚马逊 S3

答案:D

该应用程序正在使用 API 调用写入文件，这意味着它将与使用 REST API 的 Amazon S3 兼容。S3 是可大规模扩展的基于密钥的对象存储，非常适合允许从许多实例并行访问文件。Amazon S3 也将是最具成本效益的选择。使用 AWS 定价计算器进行的粗略计算显示了 EBS、EFS 和 S3 Standard 上 1TB 存储之间的成本差异。

<b>Amazon Elastic Block Store (EBS)</b> Region: US East (Ohio)	<input type="button" value="Edit"/> <input type="button" value="Action ▾"/>
<b>Amazon Elastic Block Storage (EBS)</b> <small>Number of instances (1), Average duration each instance runs (750 hours per month), Storage amount (1 TB), Snapshot Frequency (2x Daily), Amount charged per snapshot (2 GB)</small>	Monthly: 158.09 USD
<b>Amazon Elastic File System (EFS)</b> Region: US East (Ohio)	<input type="button" value="Edit"/> <input type="button" value="Action ▾"/>
<small>Data stored in Standard storage (1 TB per month)</small>	Monthly: 307.20 USD
<b>Amazon Simple Storage Service (S3)</b>	<input type="button" value="Edit"/> <input type="button" value="Action ▾"/>
<small>S3 Standard storage (1 TB per month)</small>	Monthly: 24.45 USD

正确：“Amazon S3”是正确的答案。

不正确：“Amazon EFS”是不正确的，因为它确实提供了来自许多 EC2 Linux 实例的并发访问，但这不是最具成本效益的解决方案。错误：“Amazon EBS”不正确。对于从许多 EC2 实例进行并发访问而言，弹性块存储（EBS）并不是一个好的解决方案，也不是最具成本效益的选择。将 EBS 卷安装到单个实例上，但使用多重连接是一项新功能，并且具有多个约束条件时除外。

错误：“Amazon EC2 实例存储”不正确，因为这是一个临时存储解决方案，这意味着在断电时数据会丢失。

因此，这不是长期数据存储的选择。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html> 使用我们针对考试的备忘单节省时间：

[https://digitalcloud.training/certification-training/aws-solutions-architect-associate / storage / amazon-s3 /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/)

**Q109.** 发生灾难时，公司的应用程序在单个区域的 Amazon EC2 实例上运行，解决方案架构师需要确保资源也可以部署到第二个区域。

解决方案架构师应采取哪种行动组合来完成此任务？（选择两个）

- A. 分离 EC2 实例上的卷并将其复制到 Amazon S3
- B. 从新区域中的 Amazon 机器映像（AMI）启动新的 EC2 实例
- C. 在新区域中启动新的 EC2 实例并将卷从 Amazon S3 复制到新实例
- D. 复制 EC2 实例的 Amazon Machine Image（AMI）并为目标指定其他区域
- E. 从 Amazon S3 复制 Amazon Elastic Block Store（Amazon EBS）卷并使用该 EBS 卷在目标区域中启动 EC2 实例

答案：BD

Q110. 解决方案架构师正在设计两层 Web 应用程序。该应用程序由公共子网中的 Amazon EC2 托管的面向公众的 Web 层组成。数据库层由在私有子网中的 Amazon EC2 上运行的 Microsoft SQL Server 组成。安全性是公司的首要任务。

在这种情况下应如何配置安全组？（选择两个）

- A. 配置 Web 层的安全组以允许端口 0.0.0.0/70 上的端口 443 上的入站流量
- B. 配置 Web 层的安全组以允许端口 0.0.0.0/0 上的端口 443 上的出站流量
- C. 为数据库层配置安全组，以允许来自 Web 层安全组的端口 1433 上的入站流量
- D. 配置数据库层的安全组，以允许端口 443 和 1433 上的出站流量到达 Web 层的安全组
- E. 为数据库层配置安全组，以允许来自 Web 层安全组的端口 443 和 1433 上的入站流量

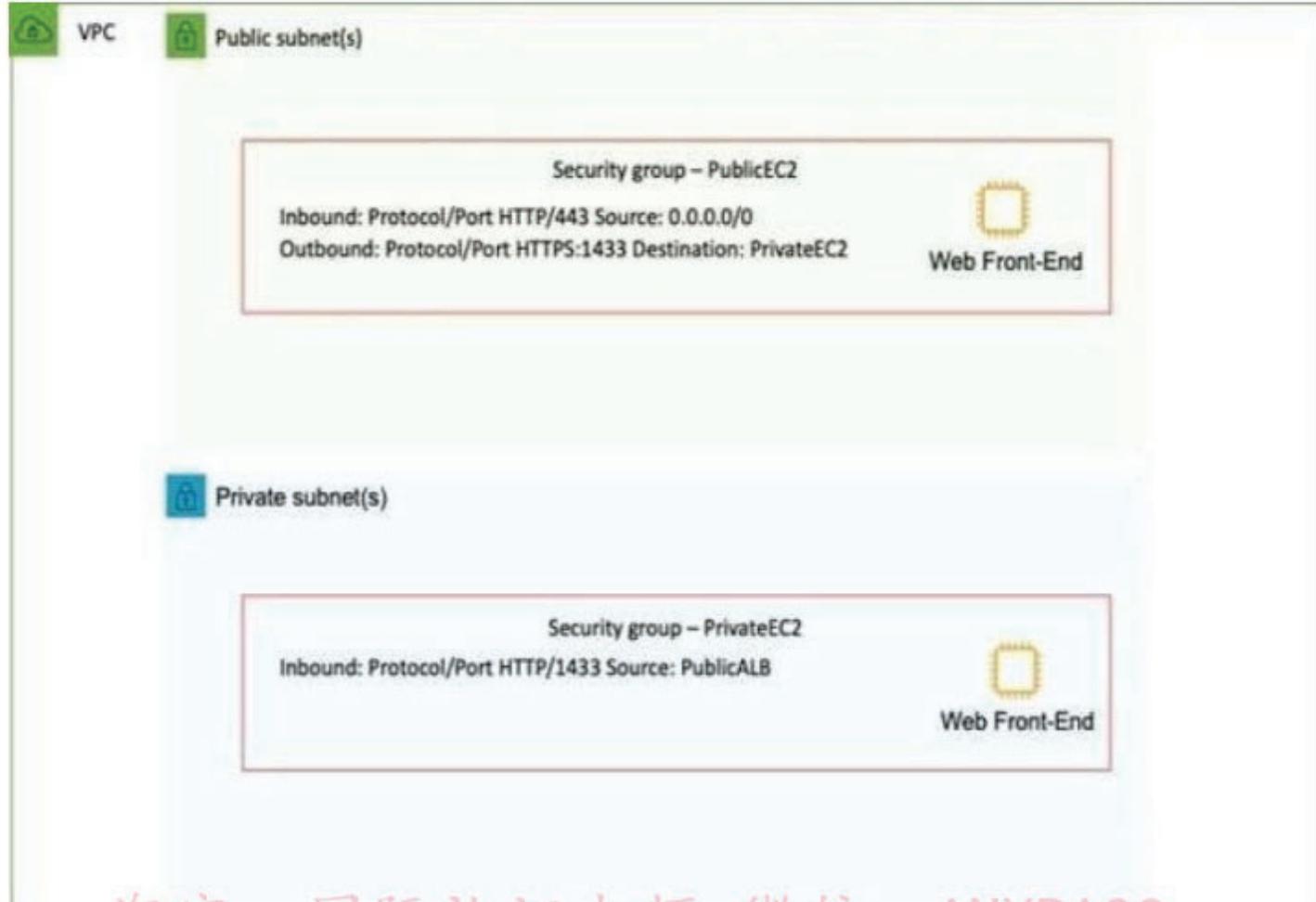
答案:AC

在这种情况下，需要一个入站规则以允许从任何 Internet 客户端到 **SSL / TLS 端口 443 上的 Web 前端** 的通信。因此，源应设置为 0.0.0.0/0 以允许任何入站通信。

为了保护从 Web 前端到数据库层的连接的安全，应从公共 EC2 安全组创建出站规则，并以私有 EC2 安全组为目标。对于 MySQL，端口应设置为 1433。私有 EC2 安全组还需要允许来自公共 EC2 安全组的 1433 端口入站流量。

可以在图中看到此配置：

淘宝：国际认证大师 微信：ANYPASS



淘宝：国际认证大师 微信：ANYPASS

正确的：“配置 Web 层的安全组以允许端口 0.0.0.0/0 上的端口 443 上的入站流量”是正确的答案。  
 正确：“将数据库层的安全组配置为允许来自 Web 层的安全组的端口 1433 上的入站流量”也是正确的答案。  
 不正确：“配置 Web 层的安全组以允许端口 0.0.0.0/0 上的端口 443 上的出站流量”不正确，因为它是反向配置的。  
 错误：“将数据库层的安全组配置为允许端口 443 和 1433 上的出站流量到达 Web 层的安全组”是不正确的，因为 MySQL 数据库实例不需要在这两个端口中的任何一个上发送出站流量。  
 错误：“配置数据库层的安全组，以允许来自 Web 层安全组的端口 443 和 1433 上的入站流量”

参考文献：

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html) 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

**Q111** 数据科学团队需要存储以进行每晚日志处理。日志的大小和数量是未知的，并将仅保留 24 小时。

什么是最具成本效益的解决方案？

A. 亚马逊 S3 冰川

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- B.Amazon S3 标准
- C.Amazon S3 智能分层
- D.Amazon S3 一区不频繁访问(S3 One Zone-IA)

答案:B

在这种情况下, **S3 标准是短期存储解决方案的最佳选择.** 在这种情况下, 日志的大小和数量是未知的, 并且在此阶段很难全面评估访问模式. 因此, 最好使用 S3 标准, 因为它具有成本效益, 可以立即访问**并且没有检索费用或每个对象的最小容量费用.**

正确: “Amazon S3 Standard”是正确的答案.

不正确: “Amazon S3 Intelligent-Tiering”是不正确的, 因为使用**此服务需要支付额外费用,** 并且对于短期需求而言, 这可能无益. 错误: “Amazon S3 一次区域不频繁访问 (S3 一次区域-IA)” 是不正确的, 因为此存储类别的每个对象的最小容量费用 (128 KB) 和每 GB 检索费用. 不正确: “Amazon S3 Glacier Deep Archive”不正确, 因为此存储类用于归档数据. **收取检索费用, 从档案中检索数据需要花费数小时**

参考文献:

<https://aws.amazon.com/s3/storage-classes/>

使用我们特定于考试的备忘单节省时间:

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-s3 />

**Q112.** 一家公司正在使用单个 Amazon EC2 实例在 AWS 上托管 Web 应用程序, 该实例将用户上传的文档存储在 Amazon EBS 卷中. 为了获得更好的可伸缩性和可用性, 该公司复制了体系结构, 并在另一个可用区中创建了第二个 EC2 实例和 EBS 卷: 将两者都放置在 Application Load Balancer 之后.

完成此更改后, 用户报告说, 每次刷新网站时, 他们可以看到其文档的一个子集或另一个, 但是却无法同时看到所有文档. 解决方案架构师应提出什么建议以确保用户一次看到所有文档"

- A. 复制数据, 以便两个 EBS 卷都包含所有文档.
  - B. 配置应用程序负载平衡器以将用户与文档一起引导到服务器.
  - C. 将数据从两个 EBS 卷复制到 Amazon EFS.
  - 修改应用程序以将新文档保存到 Amazon EPS.
  - D. 配置应用程序负载平衡器以将请求发送到两个服务器.
- 从正确的服务器返回每个文档.

答案:C

**Q113.** 您正在为数据仓库解决方案构建基础结构, 并且提出了额外的要求, 即始终有大量业务报告查询在运行, 并且您不确定当前的数据库实例是否能够处理它. 最好的解决方案是什么?

- A. 数据库参数组
- B. 阅读副本
- C. 多可用区数据库实例部署
- D. 数据库快照

答案:B

通过只读副本，可以轻松利用 MySQL 的内置复制功能来弹性扩展到单个数据库实例的容量限制之外，以处理读取繁重的数据库工作负载。在多种情况下，为给定的源数据库实例部署一个或多个只读副本可能很有意义。部署只读副本的常见原因包括：

扩展到单个数据库实例的计算或 I/O 能力之外，以处理读取繁重的数据库工作负载。多余的读取流量可以定向到一个或多个读取副本。源数据库实例不可用时提供读取流量。如果您的源数据库实例不能接受 I/O 请求（例如，由于备份或计划维护的 I/O 挂起），则可以将读取流量定向到只读副本。对于此用例，请记住，由于源数据库实例不可用，只读副本上的数据可能是“过时的”。业务报告或数据仓库方案：您可能希望业务报告查询针对只读副本而不是主生产数据库实例运行。

参考：<https://aws.amazon.com/rds/faqs/>

Q114. 在 DynamoDB 中，您可以使用 IAM 授予对 Amazon DynamoDB 资源和 API 操作的访问权限吗？

- A. 在 DynamoDB 中，无需授予访问权限
- B. 取决于访问类型
- C. 没有
- D. 是的

答案:D

淘宝：国际认证大师 微信：ANYPASS

Amazon DynamoDB 与 AWS Identity and Access Management (IAM) 集成。您可以使用 AWS IAM 授予对 Amazon DynamoDB 资源和 API 操作的访问权限。为此，您首先要编写一个 AWS IAM 策略，该文档明确列出了您要授予的权限。然后，您将该策略附加到 AWS IAM 用户或角色。

参考：<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/UsingIAMWithDDB.html>

Q115. 公司的许多数据不需要经常访问，并且可能需要花费几个小时才能检索，因此将其存储在 Amazon Glacier 上。但是，您组织中的某人表示担心他的数据比其他数据更敏感，并且想知道他知道的 S3 上的高级加密是否也用于便宜得多的 Glacier 服务上。关于此问题，以下哪种说法最适用？

- A. Amazon Glacier 上没有加密，这就是为什么它更便宜。
- B. Amazon Glacier 使用比 Amazon S3 少的加密方法使用 AES-128 自动加密数据，但是如果您愿意支付更多费用，则可以将其更改为 AES-256。
- C. Amazon Glacier 与 Amazon S3 一样，使用 AES-256 自动加密数据。
- D. Amazon Glacier 使用 AES-128 自动加密数据，这是一种比 Amazon S3 少的加密方法。

答案:C

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

与 Amazon S3 类似，Amazon Glacier 服务提供了低成本，安全和持久的存储。但是，在 S3 设计用于快速检索的情况下，Glacier 旨在用作不经常访问的数据的归档服务，并且其检索时间为几个小时是合适的。Amazon Glacier 使用 AES-256 自动加密数据，并以不可变形式持久存储数据。

Amazon Glacier 旨在为归档文件提供 99.999999999% 的平均年度耐久性。它将每个档案存储在多个设施和多个设备中。与可能需要费力的数据验证和手动修复的传统系统不同，Glacier 执行定期，系统的数据完整性检查，并且构建为可自动自我修复。参考：

<http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf>

**Q116.** 您的 EBS 量似乎未达到预期的效果，并且您的团队负责人已要求您考虑改善其性能。以下哪项不是与您的 EBS 卷的性能有关的真实陈述？

- A. 频繁快照可提供更高级别的数据持久性，并且在快照进行过程中不会降低应用程序的性能。
- B. 通用（SSD）和预配置 IOPS（SSD）卷的吞吐量限制为每个卷 128 MB / s。
- C. 您的 EBS 卷的最大性能，为它们驱动的 I/O 量与完成每个事务所花费的时间之间存在关系。
- D. 首次访问新创建或恢复的 EBS 卷上的每个数据块时，IOPS 降低了 5% 到 50%

答案:A

几个因素会影响 Amazon EBS 卷的性能，例如实例配置，I/O 特性，工作负载需求和存储配置。频繁的快照可以提供更高级别的数据持久性，但是在快照进行过程中，它们可能会稍微降低应用程序的性能。当您拥有快速变化的数据时，这种折衷变得至关重要。尽可能计划在非高峰时间进行快照，以最大程度地减少工作负载影响。

参考：<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html>

**Q117.** 您已经创建了第一个负载均衡器，并已在负载均衡器中注册了 EC2 实例。Elastic Load Balancing 会定期对所有已注册的 EC2 实例执行运行状况检查，并自动将所有传入的请求分配到已注册的健康 EC2 实例中的负载均衡器的 DNS 名称。默认情况下，负载平衡器使用\_\_\_\_协议检查实例的运行状况。

- A. HTTPS
- B. HTTP
- C. ICMP
- D. IPv6

答案:B

在 Elastic Load Balancing 中，运行状况配置使用诸如协议，Ping 端口，Ping 路径（URL），响应超时时间和运行状况检查间隔之类的信息来确定向负载均衡器注册的实例的运行状况。

当前，端口 80 上的 HTTP 是默认的运行状况检查。

参考：

<http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html>

**Q118.** 一家大型财务组织已聘请您的公司来建立大型数据挖掘应用程序. 使用 AWS, 您可以确定为此的最佳服务是您知道使用 Hadoop 的 Amazon Elastic MapReduce (EMR) . 以下哪个语句最能描述 Hadoop?

- A. Hadoop 是可以使用 AMI 安装的第三方软件
- B. Hadoop 是一个开源 python Web 框架
- C. Hadoop 是一个开源 Java 软件框架
- D. Hadoop 是一个开源 javascript 框架

答案:C

Amazon EMR 使用 Apache Hadoop 作为其分布式数据处理引擎. Hadoop 是一种开放源 Java 软件框架, 支持在大型商用硬件集群上运行的数据密集型分布式应用程序. Hadoop 实现了一个名为“MapReduce”的编程模型, 该模型将数据分为许多小工作片段, 每个小片段都可以在集群中的任何节点上执行.

该框架已被开发人员, 企业和初创企业广泛使用, 并已被证明是用于在数千个商用机器的集群上处理多达 PB 数据的可靠软件平台.

参考: <http://aws.amazon.com/elasticmapreduce/faqs/>

淘宝: 国际认证大师 微信: ANYPASS

**Q119.** 在 Amazon EC2 容器服务中, 是否支持其他容器类型?

- A.是的, EC2 容器服务支持您需要的任何容器服务.
- B.是的, EC2 容器服务还支持 Microsoft 容器服务.
- C.不, Docker 是目前 EC2 Container Service 支持的唯一容器平台.
- D.是的, EC2 容器服务支持 Microsoft 容器服务和 Openstack.

答案:C

在 Amazon EC2 容器服务中, **Docker** 是目前 EC2 容器服务支持的唯一容器平台.

参考: <http://aws.amazon.com/ecs/faqs/>

**Q120.** 解决方案架构师正在设计将在 AWS 上托管的 Web 应用程序的架构. Internet 用户将使用 HTTP 和 HTTPS 访问该应用程序.

架构师应如何设计交通管制要求?

- A.使用网络 ACL 允许 HTTP 和 HTTPS 的出站端口. 拒绝入站和出站的其他流量.
- B.使用网络 ACL 允许 HTTP 和 HTTPS 的入站端口. 拒绝入站和出站的其他流量.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

- C. 在 Web 服务器使用的安全组中允许 HTTP 和 HTTPS 的入站端口.
- D. 允许 Web 服务器使用的安全组中的 HTTP 和 HTTPS 出站端口.

答案:C

**Q121.** 解决方案架构师正在设计一个系统，以在市场关闭时分析金融市场的表现。该系统每晚将运行一系列计算密集型作业，持续 4 小时。预计完成计算作业的时间将保持不变，并且作业一旦启动就不能中断。一旦完成，该系统预计将运行至少一年。应该使用哪种类型的 Amazon EC2 实例来降低系统成本？

- A. 竞价型实例
- B. 按需实例
- C. 标准预留实例
- D. 预定的预留实例

答案:D

通过计划的预留实例（计划的实例），您可以购买以一年，一年，每天，每周或每月为基础的，具有指定开始时间和持续时间的容量预留。您预先预留了容量，以便知道在需要时可用。即使您不使用实例，也要为实例安排的时间付费。

对于不是连续运行但可以按计划运行的工作负载，计划实例是不错的选择。例如，您可以将“调度实例”用于在工作时间运行的应用程序或在周末运行的批处理。正确：“预定的预留实例”是正确的答案。不正确：“标准预留实例”不正确，因为工作负载每天仅运行 4 个小时，这会更加昂贵。

不正确：“按需实例”是不正确的，因为由于没有折扣，这将更加昂贵。

错误：“Spot Instances”不正确，因为一旦启动工作负载就无法中断。如果需要竞价价格或容量，可以使用竞价型实例终止工作负载。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / compute / amazon-ec2 />

**Q122.** 一家公司在本地托管一个静态网站，并希望将该网站迁移到 AWS。该网站应尽快为世界各地的用户加载。该公司还希望获得最具成本效益的解决方案。解决方案架构师应该怎么做才能做到这一点？

- A. 将网站内容复制到 Amazon S3 存储桶。  
配置存储桶以提供静态网页内容。  
将 S3 存储桶复制到多个 AWS 区域
- B. 将网站内容复制到 Amazon S3 存储桶。  
配置存储桶以提供静态网页内容。  
以 S3 存储桶为源配置 Amazon CloudFront
- C. 将网站内容复制到 Amazon EBS 支持的网站。

运行 Apache HTTP Server 的 Amazon EC2 实例.

配置 Amazon Route 53 地理位置路由策略以选择最接近的来源

D.将网站内容复制到多个由 Amazon EBS 支持的网站.

在多个 AWS 区域中运行 Apache HTTP Server 的 Amazon EC2 实例.

配置 Amazon CloudFront 地理位置路由策略以选择最接近的来源

答案:B

最具成本效益的选择是将网站迁移到 Amazon S3 存储桶，并配置该存储桶以进行静态网站托管。为了使全球用户获得良好的性能，解决方案架构师应随后以 S3 存储桶为源配置 CloudFront 发行版。这将在全球范围内将静态内容缓存到离用户更近的地方。正确：“将网站内容复制到 Amazon S3 存储桶。将存储桶配置为提供静态网页内容。将 Amazon CloudFront 配置为以 S3 存储桶为源”是正确的答案。

错误：“将网站内容复制到 Amazon S3 存储桶。将存储桶配置为提供静态网页内容。将 S3 存储桶复制到多个 AWS 区域”是错误的，因为此处没有将用户定向到最近区域的解决方案。如果创建了 AWS Route 53 延迟记录，这可能是一种更具成本效益（虽然不太优雅）的解决方案。错误：“将网站内容复制到 Amazon EC2 实例。配置 Amazon Route 53 地理位置路由策略以选择最接近的来源”是不正确的，因为与在 S3 上托管网站相比，使用 Amazon EC2 实例的成本效益较低。此外，仅通过一条记录就无法实现地理位置路由。

错误：“将网站内容复制到多个 AWS 区域中的多个 Amazon EC2 实例。配置 AWS Route 53 地理位置路由策略以选择最近的区域”是不正确的，因为与在 S3 上托管网站相比，使用 Amazon EC2 实例的成本效益较低。

参考文献：

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/> 通过我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/> 亚马逊云前端/

**Q123.** 解决方案架构师正在使用 Amazon S3 存储桶来实现文档审阅应用程序。

解决方案必须防止意外删除文档，并确保所有版本的文档均可用。

用户必须能够下载，修改和上传文档。应该采取哪些行动组合才能满足这些要求？（选择两个）

A.启用只读存储桶 ACL

B.在存储桶上启用版本控制

C.将 IAM 策略附加到存储桶

D.在存储桶上启用 MFA 删除

E.使用 AWS KMS 加密存储桶

答案:BD

没有一个选项为指定编写和修改对象所需的权限提供了一个好的解决方案，因此需要单独处理该要求。其他要求是为了防止意外删除，并确保文档的所有版本均可用。满足这些要求的两个解决方

案是版本控制和 MFA 删除。版本控制将保留文档每个版本的副本，多因素身份验证删除（MFA 删除）将防止意外删除，因为在尝试删除时需要提供第二个因素。正确：“在存储桶上启用版本控制”是正确的答案。正确：“在存储桶上启用 MFA 删除”也是正确的答案。错误：“在存储桶上设置只读权限”

错误：“将 IAM 策略附加到存储桶”是不正确的，因为用户需要修改文档，这也将允许删除。因此，必须实现仅控制删除的方法。

错误：“使用 AWS SSE-S3 加密存储桶”不正确，因为加密不会阻止您删除对象。

参考文献：

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

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html> 通过我们针对考试的作弊来节省时间床单：

[https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-s3 /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/)

**Q124.** 一家公司构建了一个食品订购应用程序，可以捕获用户数据并将其存储以备将来分析。该应用程序的静态前端部署在 Amazon EC2 实例上。前端应用程序将请求发送到在单独的 EC2 实例上运行的后端应用程序。

然后，后端应用程序将数据存储在 Amazon RDS 中，解决方案架构师应采取什么措施才能使架构解耦并使其可扩展”

A. 使用 Amazon S3 服务于前端应用程序，该前端应用程序将请求发送到 Amazon EC2 以执行后端应用程序。

后端应用程序将处理数据并将其存储在 Amazon RDS 中

B. 使用 Amazon S3 来服务前端应用程序，并将请求写入 Amazon Simple Notification Service (Amazon SNS) 主题。

将 Amazon EC2 实例订阅到主题的 HTTP / HTTPS 端点并处理并将数据存储在 Amazon RDS 中

C. 使用 EC2 实例服务前端并将请求写入 Amazon SQS 队列。

将后端实例放置在 Auto Scaling 组中，并根据队列深度进行扩展以在 Amazon RDS 中处理和存储数据

D. 使用 Amazon S3 服务静态前端应用程序，并将请求发送到 Amazon API Gateway，后者将请求写入 Amazon SQS 队列。

将后端实例放置在 Auto Scaling 组中，并根据队列深度进行扩展以在 Amazon RDS 中处理和存储数据

答案:D

说明

关键字：静态+解耦+可扩展

静态= S3

解耦= SQS 队列

可扩展= ASG

由于无法使用自动缩放功能，因此选项 B 将不在比赛中。由于不具备解耦功能，所以选项 A 不会出现在比赛中。由于所有 3 种组合比赛，选项 C 和 D 将参加比赛，选项 D 将是正确答案。解耦= SQS 队列；可伸缩= ASG] 和选项 C 将由于静态选项不可用而松动

参考：

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-autoscaling/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

**Q125.** 解决方案架构师必须设计一个将托管在 AWS 上的 Web 应用程序，允许用户购买对存储在 S3 存储桶中的高级共享内容的访问权。付款后，在拒绝用户访问之前，内容可以下载 14 天。以下哪一项是最简单的实现？

A. 使用具有原始访问身份 (OAI) 的 Amazon CloudFront 分发配置具有 Amazon S3 原始的分发以通过签名 URL 提供对文件的访问

设计 Lambda 函数以删除早于 14 天的数据

B. 使用 S3 存储桶并提供对图块的直接访问设计应用程序以跟踪 DynamoDB 表中的购买配置 Lambda 函数以基于对 Amazon DynamoDB 的查询来删除早于 14 天的数据

C. 将 Amazon CloudFront 分配与 OAI 一起使用

使用 Amazon S3 来源配置分发以通过签名的 URL 提供对文件的访问

将应用程序设计为使 URL 过期 14 天

D. 将 Amazon CloudFront 分配与 OAI 一起使用

使用 Amazon S3 来源配置分发以通过签名的 URL 提供对文件的访问

设计应用程序以将 URL 设置为 60 分钟的到期时间，并根据需要重新创建 URL

答案:C

**Q126.** 一家公司希望在 AWS 上托管可扩展的 Web 应用程序。来自世界不同地理区域的用户都可以访问该应用程序。应用程序用户将能够下载和上传最大为千兆字节的独特数据。开发团队需要一种经济高效的解决方案，以最大程度地减少上载和下载延迟，并最大化性能。解决方案架构师应该怎么做才能做到这一点？

A. 将 Amazon S3 与 Transfer Acceleration 一起使用以托管应用程序。

B. 使用带有 CacheControl 标头的 Amazon S3 托管应用程序。

C. 将 Amazon EC2 与 Auto Scaling 和 Amazon CloudFront 一起使用来托管应用程序。

D. 将 Amazon EC2 与 Auto Scaling 和 Amazon ElastiCache 一起使用来托管应用程序。

答案:A

**Q127.** 一家公司从多个网站捕获点击流数据，并使用批处理对其进行分析。

数据每天晚上加载到 **Amazon Redshift** 中，并由业务分析师使用。该公司希望转向近实时数据处理，以便及时了解情况。该解决方案应以最少的工作量和操作开销来处理流数据。对于该解决方案，哪种 AWS 服务组合最具有成本效益？（选择两个。）

- A.Amazon EC2
- B.AWS Lambda
- C.Amazon Kinesis 数据流
- D.Amazon Kinesis Data Firehose
- E.Amazon Kinesis 数据分析

答案:DE

A) Amazon EC2-昂贵

B) AWS lambda-非最小努力

C) Kinesis 数据流-非近实时

D) Kinesis Data Firehose-默认情况下提取数据的方式-正确 E) Kinesis Data Analytics-我们需要执行分析-CORRECT

<https://d0.awsstatic.com/whitepapers/whitepaper-streaming-data-solutions-on-aws-with-amazonkinesis.pdf> (9)

[https://aws.amazon.com/kinesis/#Evolve\\_from\\_batch\\_to\\_real-time\\_analytics](https://aws.amazon.com/kinesis/#Evolve_from_batch_to_real-time_analytics)

**Q128.** 一家公司正在将三层应用程序迁移到 AWS。该应用程序需要一个 MySQL 数据库。过去，应用程序用户报告在创建新条目时应用程序性能不佳。

这些性能问题是由于用户在工作时间内从应用程序生成不同的实时报告引起的。

哪种解决方案将在将应用程序移至 AWS 时会提高其性能？

A. 将数据导入具有预配置容量的 Amazon DynamoDB 表中。

重构应用程序以使用 DynamoDB 生成报告。

B. 在经过计算优化的 Amazon EC2 实例上创建数据库。

确保计算资源超出本地数据库。

C. 创建具有多个只读副本的 Amazon Aurora MySQL Multi-AZ 数据库集群。

为报告配置应用程序阅读器端点。

D. 创建一个 Amazon Aurora MySQL Multi-AZ 数据库集群。

配置应用程序以将群集的备份实例用作报告的端点。

答案:C

与 MySQL 兼容的 Aurora 版本可将运行在相同硬件上的标准 MySQL 的吞吐量提高 5 倍，并使现有的 MySQL 应用程序和工具无需修改即可运行。

<https://aws.amazon.com/rds/aurora/mysql-features/>

**Q129** 一家初创公司有一个基于 us-east-1 Region 的 Web 应用程序，其中多个 Amazon EC2 实例在跨多个可用区的 Application Load Balancer 后面运行。随着公司在 us-west-1 地区的用户群的增长，它需要一种具有低延迟和高可用性的解决方案。

解决方案架构师应该怎么做才能做到这一点？

A. 在 us-west-1 中配置 EC2 实例。

将应用程序负载平衡器切换到网络负载平衡器以实现跨区域的负载平衡。

B. 在 us-west-1 中配置 EC2 实例和一个 Application Load Balancer。

使负载均衡器根据请求的位置分配流量。

C. 设置 EC2 实例并在 us-west-1 中配置一个应用程序负载均衡器。

在 AWS Global Accelerator 中创建一个加速器，该加速器使用包含两个区域中的负载均衡器终端节点的终端节点组。

D. 供应 EC2 实例并在 us-west-1 中配置一个应用程序负载均衡器。

使用加权路由策略配置 Amazon Route 53。

在 Route 53 中创建指向 Application Load Balancer 的别名记录。

答案:D

“**ELB 在一个区域内提供负载平衡，AWS Global Accelerator 在多个区域提供流量管理**，通过将这些功能扩展到单个 AWS 区域之外，AWS Global Accelerator 补充了 ELB，允许您在任何区域为应用程序设置全局接口区域的数量。如果您的工作负载可以满足全球客户群的需求，我们建议您使用 AWS Global Accelerator；如果您的工作负载托管在单个 AWS 区域中，并且由同一区域内和附近的客户端使用，则可以使用应用程序负载平衡器或网络负载平衡器来管理您的资源。” <https://aws.amazon.com/global-accelerator/faqs/>

**Q130.** 一家公司计划将关键业务数据集迁移到 Amazon S3。当前的解决方案设计在 us-east-1 区域中使用单个 S3 存储桶，并启用版本控制来存储数据集。

该公司的灾难恢复策略规定，所有数据都属于多个 AWS 区域。解决方案架构师应如何设计 S3 解决方案？

A. 在另一个区域中创建另一个 S3 存储桶，并配置跨区域复制。

B. 在另一个区域中创建另一个 S3 存储桶，并配置跨域资源共享（CORS）。

C. 在另一个区域中创建另一个带有版本控制的 S3 存储桶，并配置跨区域复制。

D. 在另一个区域中创建另一个带有版本控制的 S3 存储桶，并配置跨域资源共享（CORS）。

答案:C

通过复制，可以跨 Amazon S3 存储桶自动、异步地复制对象。为对象复制配置的存储桶可以由同一 AWS 账户或不同账户拥有。您可以在不同的 AWS 区域之间或同一区域内复制对象。**源存储桶和目标存储桶都必须启用版本控制**。正确：“使用另一个区域中的版本创建其他 S3 存储桶并配置跨区域复制”是正确的答案。

错误：“在另一个区域中创建另一个 S3 存储桶并配置跨区域复制”是不正确的，因为目标存储桶也必须启用了版本控制。错误：“在另一个区域中创建其他 S3 存储桶并配置跨域资源共享（CORS）”

不正确，因为 CORS 与复制无关。错误：由于 CORS 与复制无关，因此“在另一个区域中创建具有版本控制的其他 S3 存储桶并配置跨域资源共享（CORS）”是错误的。

参考文献：

<https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-s3 />

Q131. 公司的应用程序在 VPC 的 Amazon EC2 实例上运行。应用程序之一需要调用 Amazon S3 API 来存储和读取对象。公司的安全策略限制了来自应用程序的任何 Internet 绑定流量。哪些措施可以满足这些要求并维护安全性？

- A. 配置一个 S3 接口端点。
- B. 配置一个 S3 网关端点。
- C. 在专用子网中创建一个 S3 存储桶。
- D. 在与 EC2 实例相同的 Region 中创建一个 S3 存储桶。

答案:B

#### S3 和 DynamoDB 的网关端点

<https://medium.com/tensult/aws-vpc-endpoints-introduction-ef2bf85c4422>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html> <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-gateway.html>

Q132. 公司的 Web 应用程序使用 Amazon RDS PostgreSQL 数据库实例存储其应用程序数据。在每个月初的财务结算期间，由于使用率很高，会计人员会运行大型查询，这些查询会影响数据库的性能。

该公司希望最大程度地减少报告活动对 Web 应用程序的影响。解决方案架构师应该做什么以最小的努力来减少对数据库的影响？

- A. 创建一个只读副本并将报告流量定向到该副本。
- B. 创建一个多可用区数据库，并将报告流量定向到备用数据库。
- C. 创建跨区域的只读副本，并将报告流量定向到该副本。
- D. 创建一个 Amazon Redshift 数据库并将报告流量定向到 Amazon Redshift 数据库。

答案:A

Amazon RDS 使用 MariaDB, MySQL, Oracle, PostgreSQL 和 Microsoft SQL Server 数据库引擎的内置复制功能来创建一种特殊类型的数据库实例，称为从源数据库实例的只读副本。对源数据库实例所做的更新将异步复制到只读副本。您可以通过将读取查询从应用程序路由到只读副本减轻源数据库实例的负载。

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

**Q133.** 公司必须在每个月初生成销售报告. 该报告流程在每月的第一天启动 20 个 Amazon EC2 实例. 该过程运行 7 天, 不能中断. 该公司希望将成本降到最低.  
公司应选择哪种定价模式?

- A. 预留实例
- B. 竞价块实例
- C. 按需实例
- D. 预定的预留实例

答案:D

通过计划的预留实例（计划的实例），您可以购买以一年，一年，每天，每周或每月为基础的，具有指定开始时间和持续时间的容量预留。您预先预留了容量，以便知道在需要时可用。即使您不使用实例，也要为实例安排的时间付费。

对于不是连续运行但可以按计划运行的工作负载，计划实例是不错的选择。例如，您可以将“调度实例”用于在工作时间运行的应用程序或在周末运行的批处理。

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

**Q134.** 一家公司在多个 Application Load Balancer 后面托管一个网站。该公司对其内容在世界各地具有不同的发行权。解决方案架构师需要确保为用户提供正确的内容而又不侵犯发行权。  
~~解决方案架构师应选择哪种配置来满足这些要求？~~ 微信：ANYPASS

- A. 使用 AWS WAF 配置 Amazon CloudFront.
- B. 使用 AWS WAF 配置应用程序负载平衡器.
- C. 使用地理位置策略配置 Amazon Route 53.
- D. 使用地理邻近性路由策略配置 Amazon Route 53.

答案:C

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html> (地理位置路由)

**Q135.** 公司的网站正在使用 Amazon RDS MySQL Multi-AZ 数据库实例进行事务数据存储。还有其他内部系统查询此数据库实例以获取数据以进行内部批处理。RDS 数据库实例大大降低了内部系统的数据获取速度。这会影响网站的读写性能，并且用户的响应时间会很慢。  
哪种解决方案可以改善网站的性能？

- A. 使用 RDS PostgreSQL 数据库实例而不是 MySQL 数据库.
- B. 使用 Amazon ElastiCache 缓存网站的查询响应.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- C.向当前的 RDS MySQL Multi.AZ 数据库实例添加一个额外的可用区.
- D.将一个只读副本添加到 RDS 数据库实例，并配置内部系统以查询该只读副本.

答案:D

Q136. 解决方案架构师正在为基于 Amazon Linux 的高性能计算 (HPC) 环境设计存储. 工作负载存储和处理大量需要共享存储和大量计算的工程图. 哪个存储选项将是最佳解决方案?

- A.Amazon 弹性文件系统 (Amazon EFS)
- B.适用于 Lustre 的 Amazon FSx
- C.Amazon EC2 实例存储
- D.Amazon EBS 预置的 IOPS SSD (io1)

答案:B

[https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network\\_HPC%20Storage%20Options\\_2019\\_FINAL.pdf](https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network_HPC%20Storage%20Options_2019_FINAL.pdf) (第 8 页)

Q137. 一家公司正在对 AWS 上部署的现有工作负载执行 AWS 架构完善的审查. 该审查确定了与 Microsoft Active Directory 域控制器在同一 Amazon EC2 实例上运行的面向公众的网站，该域控制器最近安装以支持其他 AWS 服务. 解决方案架构师需要推荐一种新的设计，该设计将提高体系结构的安全性并最小化对 IT 人员的管理需求. 解决方案架构师应该建议什么?

- A.使用 AWS Directory Service 创建托管 Active Directory.  
在当前 EC2 实例上卸载 Active Directory.
- B.在同一子网中创建另一个 EC2 实例，然后在其上重新安装 Active Directory.  
卸载 Active Directory.
- C.使用 AWS Directory Service 创建 Active Directory 连接器.  
对当前 EC2 实例上运行的 Active 域控制器的代理 Active Directory 请求.
- D.通过安全性声明标记语言(SAML)2.0 联合与当前 Active Directory 控制器一起启用 AWS Single Sign-On (AWS SSO).  
修改 EC2 实例的安全组以拒绝对 Active Directory 的公共访问.

答案:A

将 AD 迁移到 AWS Managed AD，并使 Web 服务器保持独立. .降低风险=从该 EC2 中删除 AD. 最小化管理员=从任何 EC2 中删除 AD  
->使用 AWS 目录服务

Active Directory 连接器仅适用于 ON-PREM AD. 它们已经存在于云中.

**Q138** . 一家公司在没有虚拟化计算资源的小型数据柜内的分支机构中运行应用程序. 应用程序数据存储在 **NFS** 卷上. 遵从性标准要求每天对 **NFS** 卷进行异地备份. 哪种解决方案满足这些要求?

- A. 在本地安装一个 AWS Storage Gateway 文件网关, 以将数据复制到 Amazon S3.
- B. 在内部安装一个 AWS Storage Gateway 文件网关硬件设备, 以将数据复制到 Amazon S3.
- C. 在内部安装带有存储卷的 AWS Storage Gateway 卷网关, 以将数据复制到 Amazon S3.
- D. 在本地安装具有缓存卷的 AWS Storage Gateway 卷网关, 以将数据复制到 Amazon S3.

答案 A

说明

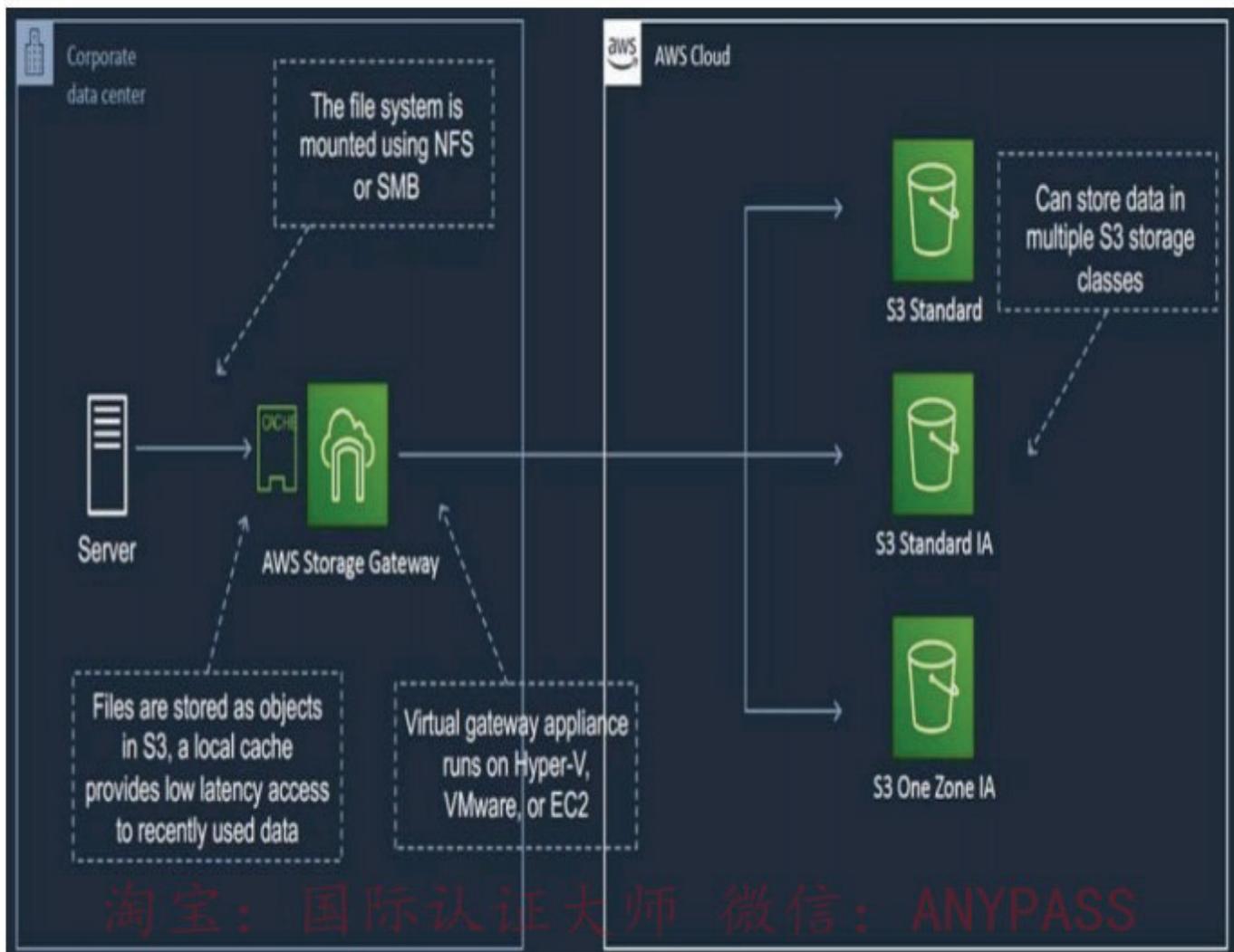
关键字: **NFS**+合规性

文件网关提供了一个虚拟的本地文件服务器, 使您可以将文件作为对象存储和检索在 Amazon S3 中. 它可用于本地应用程序以及需要在 S3 中存储文件以用于基于对象的工作负载的 Amazon EC2 驻留应用程序. 仅用于平面文件, 直接存储在 S3 上. 文件网关通过本地缓存提供对 Amazon S3 中数据的基于 **SMB** 或 **NFS** 的访问.

文件网关

AWS 存储网关

淘宝: 国际认证大师 微信: ANYPASS



下表显示了可用的不同网关以及接口和用例：

New Name	Old Name	Interface	Use Case
File Gateway	None	NFS, SMB	Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount points
Volume Gateway Stored Mode	Gateway-Stored Volumes	iSCSI	Asynchronous replication of on-prem data to S3
Volume Gateway Cached Mode	Gateway-Cached Volumes	iSCSI	Primary data stored in S3 with frequently accessed data cached locally on-prem
Tape Gateway	Gateway-Virtual Tape Library	iSCSI	Virtual media changer and tape library for use with existing backup software

存储网关概述

淘宝：国际认证大师 微信：ANYPASS

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS



正确：“在本地安装 AWS Storage Gateway 文件网关硬件设备以将数据复制到 Amazon S3”是正确的答案。

错误：“在场所安装 AWS Storage Gateway 文件网关以将数据复制到 Amazon S3”不正确。

错误：“在本地安装具有存储卷的 AWS Storage Gateway 卷网关，将数据复制到 Amazon S3”是不正确的，**因为不支持 NFS** 错误：“在本地安装具有缓存卷的 AWS Storage Gateway 卷网关以将数据复制到 Amazon S3”是不正确的，因为不支持 NFS.

参考文献：

<https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/>

<https://d0.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-混合架构.pdf>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

**Q139.** AWS 上托管的应用程序遇到性能问题，应用程序供应商希望对日志文件进行分析以进一步排除故障。日志文件存储在 Amazon S3 上，大小为 10 GB。  
应用程序所有者将在有限的时间内使日志文件对供应商可用。  
最安全的方式是什么？

- A. 启用对 S3 对象的公共读取，并提供到供应商的链接。
- B. 将文件上传到 Amazon WorkDocs 并与供应商共享公共链接。
- C. 生成一个预签名的 URL，并让供应商在日志文件过期之前下载该日志文件。
- D. 为供应商创建一个 IAM 用户，以提供对 S3 存储桶和应用程序的访问。

强制执行多因素身份验证。

答案:C

**Q140.** 一家公司在 AWS 上托管其产品信息网页。现有解决方案在 Auto Scaling 组的 Application Load Balancer 后面使用多个 Amazon C2 实例。  
该网站还使用自定义 DNS 名称，并且仅使用专用 SSL 证书与 HTTPS 通信。  
该公司正在计划推出新产品，并希望确保来自世界各地的用户在新网站上获得最佳体验。解决方案架构师应该怎么做才能满足这些要求？

- A. 重新设计应用程序以使用 Amazon CloudFront。
- B. 重新设计应用程序以使用 AWS Elastic Beanstalk。
- C. 重新设计应用程序以使用网络负载平衡器。
- D. 重新设计应用程序以使用 Amazon S3 静态网站托管。

答案:A

**Q141.** 解决方案架构师观察到，在达到所需的 Amazon EC2 容量之前，夜间批处理作业会自动扩大 1 小时。每天晚上的峰值容量是相同的，并且批处理作业始终在凌晨 1 点开始。解决方案架构师需要找到一种经济高效的解决方案，以便快速达到所需的 EC2 容量，并允许 Auto Scaling 组在批处理作业完成后按比例缩小规模。解决方案架构师应怎么做才能满足这些要求？

- A. 增加 Auto Scaling 组的最小容量。
- B. 增加 Auto Scaling 组的最大容量。
- C. 配置计划的缩放比例以扩展到所需的计算级别。
- D. 更改扩展策略以在每次扩展操作期间添加更多 EC2 实例。

答案:C

**Q142.** 一家电子商务公司正在 AWS 上运行多层应用程序。前端和后端层均在 Amazon EC2 上运行。并且数据库在 Amazon RDS for MySQL 上运行。后端层与 RDS 实例进行通信。经常需要从数据库返回相同的数据集，这会导致性能下降。应该采取什么措施来提高后端的性能？

- A. 实施 Amazon SNS 来存储数据库调用。
- B. 实现 Amazon ElastiCache 以缓存大型数据集。

- C.为 MySQL 只读副本实现 RDS 以缓存数据库调用.
- D.实施 Amazon Kinesis Data Firehose 以将调用流式传输到数据库.

答案:B

**Q143.** 托管在 Amazon EC2 实例上的公司的应用程序需要访问 Amazon S3 存储桶. 由于数据敏感性, 流量无法穿越 Internet. 解决方案架构师应如何配置访问权限?

- A.使用 Amazon Route 53 创建一个私有托管区域.
- B.在 VPC 中为 Amazon S3 配置 VPC 网关终端节点.
- C.在 EC2 实例和 S3 存储桶之间配置 AWS PrivateLink.
- D.在 VPC 和 S3 存储桶之间建立站点到站点 VPN 连接.

答案:B

**Q144.** 应用程序在专用子网中的 Amazon EC2 实例上运行. 该应用程序需要访问 Amazon DynamoDB 表. 在确保流量不会离开 AWS 网络的同时, 最安全的表访问方式是什么?

- A.将 VPC 端点用于 DynamoDB.
- B.在公共子网中使用 NAT 网关.
- C.在专用子网中使用 NAT 实例.
- D.使用连接到 VPC 的 Internet 网关.

答案:A

淘宝：国际认证大师 微信：ANYPASS

说明

关键字：专用子网+应用程序需要访问 DynamoDB

条件：流量不会离开 AWS 网络

DynamoDB = VPC Endpoint / VPC 网关端点

选项-A-赢得胜利, 它可以使用区域间 VPC 对等安全地跨 AWS 区域访问 AWS PrivateLink 端点  
选项-B-超出比赛条件, 不符合条件  
选项-C-超出比赛条件, 不符合条件. 选项-D-超出比赛条件, 不符合条件.

VPC 预约

接口终端节点使用 AWS PrivateLink, 并且是具有专用 IP 地址的弹性网络接口 (ENI), 用作专用于受支持服务的流量的入口点.

使用 PrivateLink, 您可以将 VPC 连接到支持的 AWS 服务, 其他 AWS 账户托管的服务 (VPC 终端服务) 以及支持的 AWS Marketplace 合作伙伴服务.

通过区域间 VPC 对等进行 AWS PrivateLink 访问:

AWS VPC 中的应用程序可以跨 AWS 安全访问 AWS PrivateLink 终端节点

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

使用区域间 VPC 对等的区域.

AWS PrivateLink 允许您以高可用性私有访问 AWS 上托管的服务和可扩展的方式，而无需使用公共 IP，也不需要流量通过 Internet. 客户可以私下连接到服务，即使服务端点位于其他位置

AWS 区域.

使用区域间 VPC 对等传输的流量保持在全局 AWS 主干网上，并且永远不会经过公共互联网.

网关端点是网关，它是路由表中指定路由的目标，用于用于发往受支持的 AWS 服务的流量.

接口 VPC 终结点（接口终结点）使您可以连接到由以下设备提供支持的服务

AWS PrivateLink.

下表突出显示了有关两种端点类型的一些关键信息：

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

参考文献：

[https://aws.amazon.com/vpc/?nc2=h\\_ql\\_prod\\_nt\\_avpc](https://aws.amazon.com/vpc/?nc2=h_ql_prod_nt_avpc)

<https://youtu.be/jZAvKgqlrjY>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

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

**Q145.** 解决方案架构师需要为使用自定义域名的用户访问的静态单页应用程序设计低延迟解决方案. 该解决方案必须是无服务器的, 在传输过程中经过加密且具有成本效益.

解决方案架构师应使用哪种 AWS 服务和功能组合? (选择两个.)

- A. 亚马逊 S3
- B. 亚马逊 EC2
- C. AWS Fargate
- D. Amazon CloudFront
- E. 弹性负载平衡器

答案:AD

**Q146.** 公司有全球用户访问部署在不同 AWS 区域中的应用程序, 从而公开了公共静态 IP 地址. 通过 Internet 访问应用程序时, 用户体验很差.

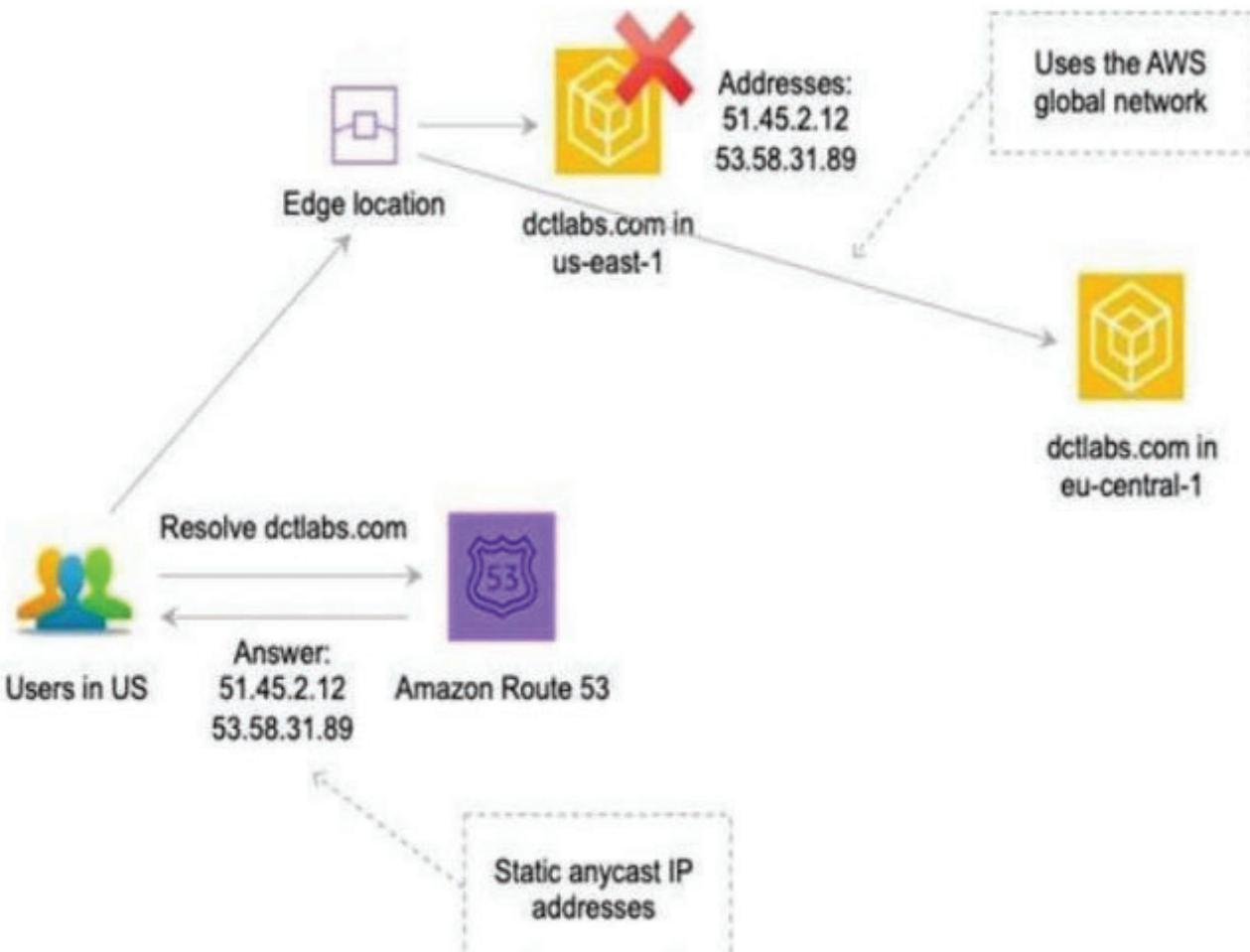
解决方案架构师应建议什么以减少 Internet 延迟?

- A. 设置 AWS Global Accelerator 并添加终端节点.
- B. 在多个区域中设置 AWS Direct Connect 位置.
- C. 设置一个 Amazon CloudFront 发行版以访问应用程序.
- D. 设置 Amazon Route 53 地理接近路由策略以路由流量.

答案:C

AWS Global Accelerator 是一项服务, 您可以在其中创建加速器, 以提高本地和全局用户的应用程序的可用性和性能. Global Accelerator 将流量引导到 AWS 全局网络上的最佳端点. 这可以提高全球受众使用的 Internet 应用程序的可用性和性能. Global Accelerator 是一项全局服务, 支持 AWS 区域表中列出的多个 AWS 区域中的终端节点.

默认情况下, Global Accelerator 为您提供与您的加速器关联的两个静态 IP 地址. (或者, 也可以不使用 Global Accelerator 提供的 IP 地址, 而是将这些入口点配置为来自您自己带到 Global Accelerator 的 IP 地址范围内的 IPv4 地址.)



淘宝：国际认证大师 微信：ANYPASS

静态 IP 地址是从 AWS 边缘网络播送的，并在多个 AWS 区域中的多个终端资源之间分配传入应用程序流量，从而提高了应用程序的可用性。端点可以是网络负载平衡器，应用程序负载平衡器，EC2 实例或位于一个 AWS 区域或多个区域中的弹性 IP 地址。

正确：“设置 AWS Global Accelerator 并添加终端节点”是正确的答案。错误：“在多个区域中设置 AWS Direct Connect 位置”不正确，因为这是用于从本地数据中心连接到 AWS 的。对于未连接到本地数据中心的用户，它不会提高性能。错误：“设置 Amazon CloudFront 分发以访问应用程序”不正确，因为 **CloudFront 无法公开静态公共 IP 地址**。

错误：“设置 Amazon Route 53 地理接近路由策略以路由流量”是不正确的，因为这不会减少 Internet 延迟，也不会使用 Global Accelerator. GA 会将用户引导到最近的边缘位置，然后使用 AWS 全球网络。

参考文献：

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html> 使用我们针对考试的备忘单节省时间：

[https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery / aws-global-accelerator /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-global-accelerator/)

**Q147.** 一个应用程序需要几年的开发环境（DEV）和生产环境（PROD）。DEV 实例将在正常工作时间内每天运行 10 个小时，而 PROD 实例将每天运行 24 小时。解决方案架构师需要确定计算实例购买策略，以最大程度地降低成本。

哪种解决方案最有效？

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- A. 具有竞价型实例的 DEV 和具有按需实例的 PROD
- B. 带按需实例的 DEV 和带竞价实例的 PROD
- C. 具有预定保留实例的 DEV 和具有保留实例的 PROD
- D. 具有按需实例的 DEV 和具有预定保留实例的 PROD

答案:C

**Q148.** 解决方案架构师正在设计面向客户的应用程序。根据一年中的时间以及全年中明确定义的访问模式，预计该应用程序的读写次数将有所不同。管理要求在 AWS 云中管理数据库审核和扩展。恢复点目标 (RPO) 必须少于 5 小时。哪些解决方案可以做到这一点？（选择两个。）

- A. 将 Amazon DynamoDB 与自动缩放一起使用。  
使用按需备份和 AWS CloudTrail。
- B. 使用具有自动扩展功能的 Amazon DynamoDB。  
使用按需备份和 Amazon DynamoDB 流。
- C. 使用 Amazon Redshift 配置并发扩展。  
启用审核日志记录。  
每 4 小时执行一次数据库快照。
- D. 将 Amazon RDS 与预置 IOPS 结合使用。  
启用数据库审核参数。  
每 5 小时执行一次数据库快照。
- E. 将 Amazon RDS 与自动缩放一起使用。  
启用数据库审核参数。  
将备份保留期配置为至少 1 天。

答案:AB

**Q149.** Amazon S3 上的一个网站。该网站每月提供 PB 级的出站流量，这占了公司大部分 AWS 成本。解决方案架构师应该怎么做才能降低成本？

- A. 使用现有网站作为源配置 Amazon CloudFront。
- B. 将网站移至带有 Amazon EBS 卷的 Amazon EC2 进行存储。
- C. 使用 AWS Global Accelerator 并指定现有网站作为终端节点。
- D. 重新设计网站，使其在 Amazon API Gateway 和 AWS Lambda 的组合上运行。

答案:A

**Q150.** 解决方案架构师创建了两个 IAM 策略：Policy1 和 Policy2。这两个策略都附加到 IAM 组。

### Policy1

```
{  
    "Version": "2012-10-17", "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iam:Get*",  
                "iam>List*",  
                "kms>List*",  
                "ec2:*",  
                "ds:*",  
                "logs:Get*",  
                "logs:Describe*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

### Policy2

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ds>Delete*",  
            "Resource": "*"  
        }  
    ]  
}
```

将云工程师作为 1AM 用户添加到 1AM 组中，云工程师将执行哪些操作？

- A. 删除 1AM 用户
- B. 删除目录
- C. 删除 Amazon EC2 实例

答案:B

**Q151.** 解决方案架构师正在帮助开发人员使用 AWS 服务设计新的电子商务购物车应用程序。开发人员不确定当前的数据库架构，并希望随着电子商务网站的发展而进行更改。该解决方案必须具有高度的弹性，并能够自动扩展读写容量。

哪个数据库解决方案满足这些要求？

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- A.Amazon Aurora PostgreSQL
- B.启用按需的 Amazon DynamoDB
- C.启用了 DynamoDB 流的 Amazon DynamoDB
- D.Amazon SQS 和 Amazon Aurora PostgreSQL

答案:B

原始答案是 A 现更正为 B

**Q152.** 解决方案架构师正在为新应用程序设计架构，该应用程序需要低网络延迟和 Amazon EC2 实例之间的高网络吞吐量。建筑设计应包括哪些组件？

- A.具有竞价型实例类型的 Auto Scaling 组.
- B.使用集群放置策略的放置组.
- C.使用分区放置策略的放置组.
- D.具有按需实例类型的 Auto Scaling 组.

答案:B

**Q153.** 公司的 Web 应用程序具有零星的使用模式。每个月初都有大量使用量，每周初有中等量使用量，一周中有不可预测的使用量。该应用程序由一个 Web 服务器和一个运行在数据中心内部的 MySQL 数据库服务器组成。该公司希望将应用程序移至 AWS Cloud，并需要选择一个经济高效的数据库平台，而无需修改数据库。

哪种解决方案可以满足这些要求？

- 淘宝店名：国际认证大师 微信：ANYPASS
- A.Amazon DynamoDB
  - B.适用于 MySQL 的 Amazon RDS
  - C.与 MySQL 兼容的 Amazon Aurora Serverless
  - D.在 Auto Scaling 组中部署在 Amazon EC2 上的 MySQL

答案:C

**Q154.** 解决方案架构师正在设计任务关键型 Web 应用程序。它由位于 Application Load Balancer 和关系数据库后面的 Amazon EC2 实例组成。该数据库应具有高可用性并具有容错能力。哪些数据库实现将满足这些要求？（选择两个。）

- A.亚马逊 Redshift
- B.亚马逊 DynamoDB
- C.Amazon RDS for MySQL
- D.与 MySQL 兼容的 Amazon Aurora Multi-AZ
- E.适用于 SQL Server 标准版 Multi-AZ 的 Amazon RDS

答案:D E

**Q155.** 一家媒体公司正在评估将其系统迁移到 AWS 云的可能性。该公司至少需要 10 TB 的存储，并具有用于视频处理的最大可能的 I/O 性能。300 TB 的非常耐用的存储空间可用于存储媒体内

容，而 900 TB 的存储空间可满足不再使用的存档媒体的要求。解决方案架构师应推荐哪些服务来满足这些要求？

- A. Amazon EBS 提供最佳性能，Amazon S3 提供持久性数据存储，Amazon S3 Glacier 提供档案存储
- B. Amazon EBS，以获得最佳性能。Amazon EFS 用于持久数据存储，Amazon S3 Glacier 用于档案存储
- C. Amazon EC2 实例存储可实现最佳性能，Amazon EFS 可实现持久数据存储，Amazon S3 可用于归档存储
- D. Amazon EC2 实例存储可实现最佳性能，Amazon S3 可实现持久数据存储，Amazon S3 Glacier 可用于归档存储

答案:A

**Q156.** 公司在 Amazon EC2 实例上托管一个应用程序，该实例最多需要 200 GB 的存储空间。该应用程序很少使用，在早晨和晚上都有高峰。磁盘 I/O 有所不同，但最高达到 3,000 IOPS。该公司的首席财务官担心成本，并已要求解决方案架构师推荐最经济高效的存储方案，而这不会牺牲性能。

解决方案架构师应建议哪种解决方案？

- A. Amazon EBS 冷硬盘 (sc1)
- B. Amazon EBS 通用 SSD (gp2)
- C. Amazon EBS 预置的 IOPS SSD (io1)
- D. Amazon EBS 吞吐量优化的硬盘 (st1)

答案:B

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。这些卷可提供单位毫秒的延迟，并能够长时间扩展至 3,000 IOPS。

在最低 100 IOPS (在 33.33 GiB 及以下) 和最大 16,000 IOPS (在 5,334 GiB 及以上) 之间，基准性能以每 GiB 的卷大小 3 IOPS 线性扩展。AWS 设计 gp2 卷以在 99% 的时间内提供其预配置性能。gp2 的大小范围可以从 1 GiB 到 16 TiB。

在这种情况下，该卷的基准性能为  $3 \times 200 = 600$  IOPS。该卷可能还会长时间突破 3,000 IOPS。随着 I/O 的变化，这应该是合适的。正确：“Amazon EBS 通用 SSD (gp2)”是正确的答案。不正确：“Amazon EBS 配置的 IOPS SSD (io1)”不正确，因为这将是一个更昂贵的选择，并且对于此工作负载的性能特征不是必需的。错误：“Amazon EBS Cold HDD (sc1)”不正确，因为没有适用于 HDD 卷的 IOPS SLA。它们可能无法很好地满足此工作负载的需求。不正确：“Amazon EBS 吞吐量优化的 HDD (st1)”不正确，因为没有针对 HDD 卷的 IOPS SLA，它们可能无法很好地应对此工作负载。

参考文献：

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html> 使用我们针对考试的备忘单节省时间：

[https://digitalcloud.training/certification-training/aws-solutions-architect- associate / compute / amazon-ebs /](https://digitalcloud.training/certification-training/aws-solutions-architect-associate / compute / amazon-ebs /)

**Q157.** 一家公司将 Amazon S3 中的文件交付给某些没有 AWS 凭证的用户. 必须为这些用户授予有限的访问权限. 解决方案架构师应该怎么做才能安全地满足这些要求?

- A. 在 Amazon S3 存储桶上启用公共访问.
- B. 生成一个预先签名的 URL 与用户共享.
- C. 使用 AWS KMS 加密文件并向用户提供密钥.
- D. 创建并分配 IAM 角色, 这些角色将向用户授予 GetObject 权限.

答案:B

**Q158** 一家租赁公司每月为其所有客户生成并通过电子邮件发送 PDF 报表. 每个语句的大小约为 400 KB. 客户可以在生成报表后的 30 天内从网站下载其报表. 在 3 年租期结束时, 会通过电子邮件向客户发送包含所有对帐单的 ZIP 文件. 对于这种情况, 最有成本效益的存储解决方案是什么?

- A. 使用 Amazon S3 Standard 存储类存储语句. 创建生命周期策略, 以在 1 天后将语句移至 Amazon S3 Glacier 存储.
- B. 使用 Amazon S3 Glacier 存储类存储语句. 创建生命周期策略, 以在 30 天后将语句移至 Amazon S3 Glacier Deep Archive 存储.
- C. 使用 Amazon S3 Standard 存储类存储语句. 创建生命周期策略, 以在 30 天后将语句移至 Amazon S3 一次区域不频繁访问 (S3 One Zone-IA) 存储.
- D. 使用 Amazon S3 Standard-Infrequent Access (S3 Standard-IA) 存储类存储语句. 创建生命周期策略, 以在 30 天后将语句移至 Amazon S3 Glacier 存储.

答案:D

**Q159.** 解决方案架构师正在将静态内容从 Amazon EC2 实例上托管的公共网站移动到 Amazon S3 存储桶. Amazon CloudFront 发行版将用于交付静态资产. EC2 实例使用的安全组将访问限制为一组有限的 IP 范围. 同样, 对静态内容的访问也应受到限制. 哪些步骤组合可以满足这些要求? (选择两个.)

- A. 创建一个原始访问身份 (OAI) 并将其与分发关联. 更改存储桶策略中的权限, 以便仅 OAI 可以读取对象.
- B. 创建一个包含与 EC2 安全组中相同的 IP 限制的 AWS WAF Web ACL. 将此新的 Web ACL 与 CloudFront 分配关联.
- C. 创建一个新的安全组, 其中包括与当前 EC2 安全组中存在的 IP 限制相同的 IP 限制. 将此新安全组与 CloudFront 分配关联.
- D. 创建一个新的安全组, 其中包括与当前 EC2 安全组中相同的 IP 限制. 将此新安全组与托管静态内容的 S3 存储桶相关联.
- E. 创建一个新的 IAM 角色, 并将该角色与分发相关联. 在 S3 存储桶或 S3 存储桶中的文件上更改权限, 以便只有新创建的 IAM 角色才具有读取和下载权限.

答案:AB

原始答案是 CE , 现更正为 AB,

**Q160.** 一家公司有一个大型 Microsoft SharePoint 部署在本地运行，需要 Microsoft Windows 共享文件存储。该公司希望将此工作负载迁移到 AWS Cloud，并正在考虑各种存储选项。存储解决方案必须具有高可用性，并且必须与 Active Directory 集成以进行访问控制。哪种解决方案可以满足这些要求？

- A. 配置 Amazon EFS 存储并设置 Active Directory 域以进行身份验证。
- B. 在两个可用区中的 AWS Storage Gateway 文件网关上创建 SMB 文件共享。
- C. 创建一个 Amazon S3 存储桶，并将 Microsoft Windows Server 配置为将其作为卷安装。
- D. 在 AWS 上为 Windows 文件服务器创建 Amazon FSx 文件系统，并设置 Active Directory 域以进行身份验证。

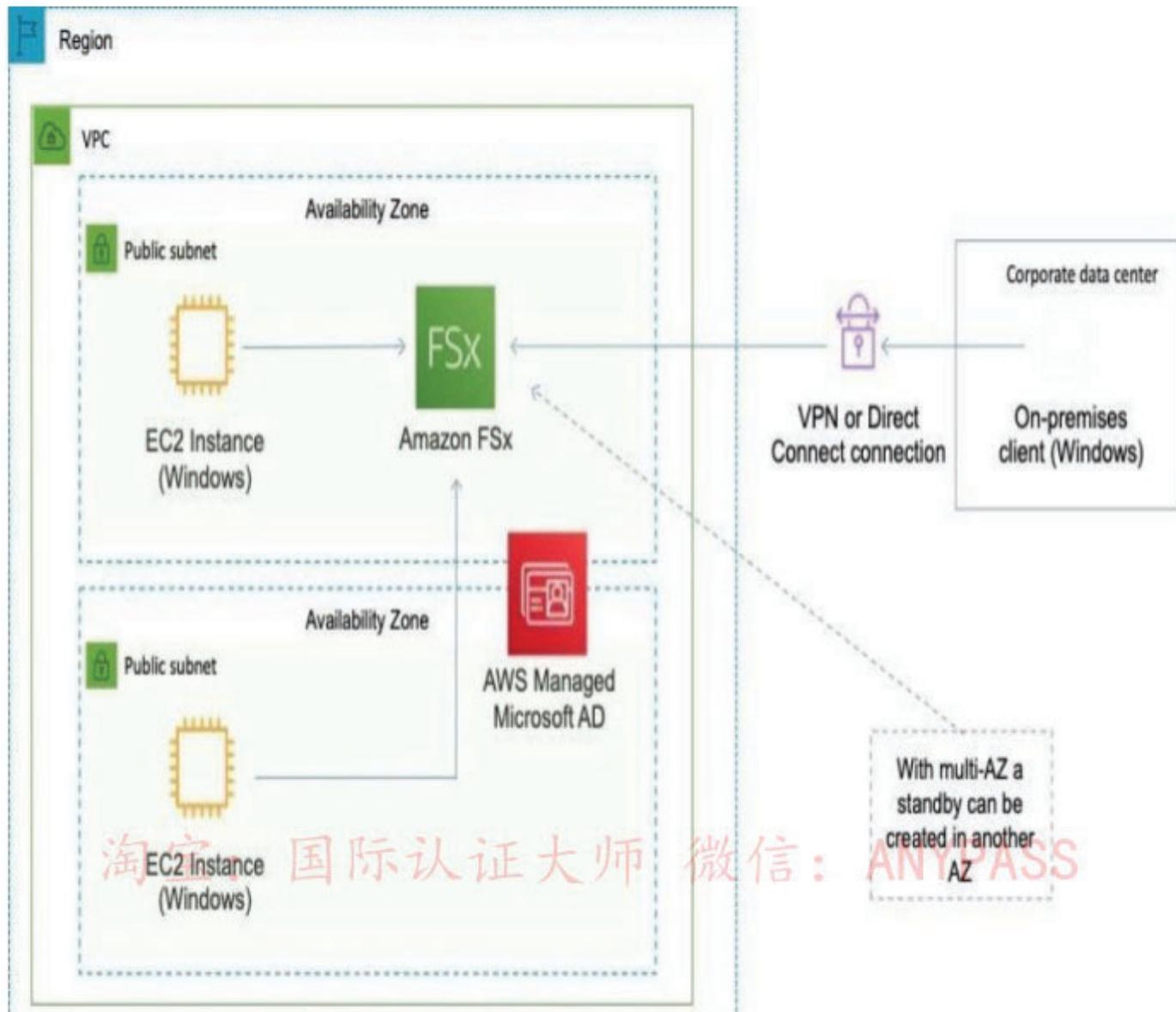
答案:D

说明

适用于 Windows 的 Amazon FSx File Server 提供了完全托管的、高度可靠的和可扩展的文件存储，可以通过行业标准的**服务器消息块 (SMB) 协议**进行访问。它基于 Windows Server 构建，提供了广泛的管理功能，例如用户配额，最终用户文件还原以及 Microsoft Active Directory (AD) 集成。它提供了单可用区和多可用区部署选项，完全托管的备份以及静态数据和传输数据的加密。您可以通过 SSD 和 HDD 存储选件来优化成本和性能，以满足工作负载的需求。您可以随时扩展存储并更改文件系统的吞吐量性能。可从 Windows, Linux 和 MacOS 计算实例以及在 AWS 或本地运行的设备访问 Amazon FSx 文件存储。

与 Microsoft Active Directory (AD) 配合使用可轻松将文件系统与 Windows 环境集成在一起。

淘宝：国际认证大师 微信：ANYPASS



正确：“Amazon FSx”是正确的答案。

错误：“Amazon EFS”不正确，因为 **EFS 仅支持 Linux 系统** 不正确：“Amazon S3”不正确，因为这不是 Microsoft 文件系统的合适替代品。

错误：“**AWS Storage Gateway**”不正确，因为此服务主要用于将本地存储连接到云存储。它由内部安装的软件设备组成，可以与 SMB 共享一起使用，但实际上将数据存储在 S3 上。它也用于迁移。但是，在这种情况下，公司需要替换文件服务器场，Amazon FSx 是此工作的最佳选择。

参考文献：

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-fsx />

**Q161.** 一家公司在 VPC 中使用使用分层目录结构的应用程序运行多个 Amazon EC2 Linux 实例。应用程序需要快速并发地对共享存储进行读写操作如何实现？

- A. 创建一个 Amazon EFS 文件系统，并从每个 EC2 实例安装它。
- B. 创建一个 Amazon S3 存储桶，并允许从 VPC 中的所有 EC2 实例进行访问。
- C. 在 Amazon EBS 配置的 IOPS SSD (io1) 卷上创建文件系统。将卷附加到所有 EC2 实例。
- D. 在附加到每个 EC2 实例的 Amazon EBS 卷上创建文件系统。在不同的 EC2 实例之间同步 Amazon EBS 卷。

答案:A

**Q162.** 一家公司使用 Amazon ECS 运行应用程序。该应用程序创建原始图像的调整大小版本，然后进行 Amazon S3 API 调用以将调整大小的图像存储在 Amazon S3 中。解决方案架构师如何确保应用程序有权访问 Amazon S3？

- A. 更新 AWS IAM 中的 S3 角色以允许从 Amazon ECS 进行读/写访问，然后重新启动该容器。
- B. 创建一个具有 S3 权限的 IAM 角色，然后在任务定义中将该角色指定为 taskRoleArn。
- C. 创建一个安全组，该安全组允许从 Amazon ECS 到 Amazon S3 的访问，并更新 ECS 集群使用的启动配置。
- D. 创建一个具有 S3 权限的 IAM 用户，然后以该帐户身份登录时重新启动 ECS 集群的 Amazon EC2 实例。

答案:B

**Q163.** 解决方案架构师已配置以下 IAM 策略。  
淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "lambda:*"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": [  
                "lambda>CreateFunction",  
                "lambda>DeleteFunction"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "IpAddress": {  
                    "aws:SourceIp": "220.100.16.0/20"  
                }  
            }  
        }  
    ]  
}
```

淘宝：国际认证大师 微信：ANYPASS

该政策将允许采取哪种行动？

- A. 可以从任何网络删除 AWS Lambda 函数.
- B. 可以从任何网络创建 AWS Lambda 函数.
- C. 可以从 100.220.0.0/20 网络中删除 AWS Lambda 函数.

答案:C

**Q164.** 一个网站运行一个 Web 应用程序，该应用程序每天中午都会收到大量流量。用户每天上传新图片和新内容，但一直抱怨超时。该架构使用 Amazon EC2 Auto Scaling 组，并且自定义应用程序始终在启动时花费 1 分钟在响应用户请求之前启动。解决方案架构师应如何重新设计架构，以更好地响应不断变化的流量？

- A. 使用慢启动配置配置网络负载均衡器.
- B. 将 AWS ElastiCache for Redis 配置为将直接请求卸载到服务器.
- C. 使用实例预热条件配置 Auto Scaling 步骤扩展策略.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

D. 将 Amazon CloudFront 配置为使用应用程序负载均衡器作为源.

答案:D

**Q165.** 一家公司的网站在两个可用区中的 Amazon EC2 实例上运行. 该公司预计特定假期的流量会激增, 并希望提供一致的用户体验. 解决方案架构师如何满足此要求?

- A. 使用逐步缩放.
- B. 使用简单缩放.
- C. 使用生命周期挂钩.
- D. 使用计划的缩放比例.

答案:D

**Q166.** 公司的 Web 应用程序在 Application Load Balancer 后面的 Amazon EC2 实例上运行. 该公司最近更改了政策, 现在要求只能从一个特定国家/地区访问该应用程序.

哪种配置可以满足此要求?

- A. 为 EC2 实例配置安全组.
- B. 在应用程序负载平衡器上配置安全组.
- C. 在 VPC 中的 Application Load Balancer 上配置 AWS WAF.
- D. 为包含 EC2 实例的子网配置网络 ACL.

答案:C

淘宝：国际认证大师 微信：ANYPASS

**Q167.** 一家公司在本地存储了 150 TB 的存档图像数据, 需要在下个月内将其修剪到 AWS 云中. 该公司当前的网络连接仅在夜间允许最多 100 Mbps 的上传. 什么是最经济有效的机制来移动这些数据并在迁移截止日期之前完成?

- A. 使用 AWS Snowmobile 将数据运送到 AWS.
- B. 订购多个 AWS Snowball 设备以将数据发送到 AWS.
- C. 启用 Amazon S3 Transfer Acceleration 并安全地上传数据.
- D. 创建一个 Amazon S3 VPC 终端节点并建立一个 VPN 以上传数据.

答案:B

**Q168.** 三层 Web 应用程序处理来自客户的订单. Web 层由位于应用程序负载平衡器后面的 Amazon EC2 实例组成, 这是一个三个 EC2 实例的中间层, 使用 Amazon SQS 与 Web 层分离. 和一个 Amazon DynamoDB 后端. 在高峰时段, 由于处理时间很长, 使用该网站提交订单的客户必须比正常等待更长的时间才能收到确认. 解决方案架构师需要减少这些处理时间. 哪种行动最有效地做到这一点?

- A. 将 SQS 队列替换为 Amazon Kinesis Data Firehose.
- B. 在 DynamoDB 后端层前面使用 Amazon ElastiCache for Redis.
- C. 添加一个 Amazon CloudFront 发行版以缓存 Web 层的响应.
- D. 使用 Amazon EC2 Auto Scaling 根据 SOS 队列深度扩展中间层实例.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

答案:D

Q169. 一家公司希望在 AWS 上托管一个 Web 应用程序，该应用程序将与 VPC 中的数据库进行通信。

该应用程序应具有很高的可用性。

解决方案架构师应该建议什么？

- A. 创建两个 Amazon EC2 实例以在负载均衡器后面托管 Web 服务器，然后在大型实例上部署数据库。
- B. 在具有多个 Web 服务器的 Auto Scaling 组的多个可用区中部署负载均衡器，然后在多个可用区中部署 Amazon RDS。
- C. 在具有用于 Web 服务器的 Auto Scaling 组的公共子网中部署负载均衡器，然后在专用子网中的 Amazon EC2 实例上部署数据库。
- D. 部署具有 Auto Scaling 组的两个 Web 服务器，配置指向两个 Web 服务器的域，然后在多个可用区中部署数据库体系结构。

答案:B

Q170. 一家公司正在迁移到 AWS 云。文件服务器是第一个要迁移的工作负载。用户必须能够使用 **服务器消息块 (SMB) 协议** 访问文件共享。哪些 AWS 托管服务符合这些要求？

- A. 亚马逊 EBS
- B. 亚马逊 EC2
- C. Amazon FSx
- D. 亚马逊 S3

答案:C

说明

适用于 Windows 的 Amazon FSx File Server 提供了完全托管的，高度可靠的文件存储，可通过行业标准的服务器消息块 (SMB) 协议进行访问。

Amazon FSx 构建在 Windows Server 上，并提供了丰富的管理功能集，其中包括最终用户文件还原，用户配额和访问控制列表 (ACL)。

此外，适用于 Windows 文件服务器的 Amazon FSX 在单可用区和多可用区部署中均支持分布式文件系统复制 (DFSR)，如下面的功能比较表所示。

正确：“Amazon FSx”是正确的答案。

错误：“Amazon Elastic Block Store (EBS)”不正确。EFS 和 EBS 不是此解决方案的好用例。两种存储解决方案都无法将 Amazon S3 对象作为文件呈现给应用程序。

不正确：“Amazon EC2”不正确，因为没有 SMB 支持。不正确：“Amazon S3”不正确，因为这不是 Microsoft 文件系统的合适替代品。

参考文献：

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

**Q171.** 一家公司拥有一个移动聊天应用程序，该应用程序具有基于 Amazon DynamoDB 的数据存储。用户希望以尽可能少的延迟读取新消息。解决方案架构师需要设计一个需要最少应用程序更改的最佳解决方案。

解决方案架构师应选择哪种方法？

- A. 为新消息表配置 Amazon DynamoDB Accelerator (DAX)。更新代码以使用 DAX 端点。
- B. 添加 DynamoDB 只读副本以处理增加的读取负载。更新应用程序以指向只读副本的读取端点。
- C. 将 DynamoDB 中新消息表的读取容量单位增加一倍。继续使用现有的 DynamoDB 端点。
- D. 将 Amazon ElastiCache for Redis 缓存添加到应用程序堆栈。更新应用程序以指向 Redis 缓存端点，而不是 DynamoDB。

答案:A

说明

Amazon DynamoDB Accelerator(DAX)是一个完全托管的,高度可用的内存缓存 可以将 Amazon DynamoDB 响应时间从毫秒减少到微秒，甚至每秒数百万个请求也是如此。



Amazon ElastiCache 是 不正确的，因为尽管您可以将 ElastiCache 用作数据库缓存，但与 DynamoDB DAX 相比，它不会将 DynamoDB 响应时间从毫秒减少到微秒。

AWS Device Farm 是不正确的，因为这是一项应用程序测试服务，可让您立即在许多设备上测试您的 Android, iOS 和 Web 应用程序并与之交互，或实时再现设备上的问题。

**DynamoDB 只读副本不正确，因为它主要用于自动执行表和全局二级索引的容量管理。**

参考文献：

<https://aws.amazon.com/dynamodb/dax>

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

查看此 Amazon DynamoDB 备忘单：

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

<https://tutorialsdojo.com/aws-cheat-sheet-amazon-dynamodb/>

**Q172.** 一家公司希望将 AWS 区域用作其本地基础架构的灾难恢复位置。该公司拥有 10 TB 的现有数据，而内部数据中心具有 1 Gbps 的互联网连接。解决方案架构师必须找到一个解决方案，以便公司在 72 小时内将其现有数据存储在 AWS 上，而无需使用未加密的通道进行传输。解决方案架构师应选择哪种解决方案？

- A. 使用 FTP 将最初的 10 TB 数据发送到 AWS。
- B. 使用 AWS Snowball 将最初的 10 TB 数据发送到 AWS。
- C. 在 Amazon VPC 与公司的数据中心之间建立 VPN 连接。
- D. 在 Amazon VPC 与该公司的数据中心之间建立 AWS Direct Connect 连接。

答案:C

关键字：AWS 区域作为本地 DC 的 DR（现有数据= 10TB）+ 1G Internet 连接

条件：72 小时内在 AWS 上 10 TB + 没有未加密的频道

没有未加密的通道= VPN

FTP =未加密的频道

选项-A-非竞赛，因为这是未加密的频道且不符合条件。选项-B-由于时间限制的目标和订单/交付/AWS Snowball 设备交付而超出竞赛

选项-C-竞赛胜利，使用现有的 1G Internet Link，我们可以使用加密的通道在 24 小时内传输 10TB 数据

选项-D-由于时间限制的目标和订单/交货/交付 AWS Direct Connect 将花费时间

参考文献：

<https://docs.aws.amazon.com/snowball/latest/ug/mailin-storage.html>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery / aws-direct-connect />

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery / amazon-vpc />

<https://tutorialsdojo.com/aws-direct-connect/>

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

**Q173.** Web 应用程序在 Application Load Balancer 后面的 Amazon EC2 实例上运行。该应用程序允许用户创建历史天气数据的自定义报告。生成报告最多可能需要 5 分钟。这些长时间运行的请求使用许多可用的传入连接，从而使系统对其他用户无响应。解决方案架构师如何使系统更具响应能力？

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- A. 将 Amazon SQS 与 AWS Lambda 一起使用可生成报告.
- B. 将应用程序负载平衡器上的空闲超时增加到 5 分钟.
- C. 更新客户端应用程序代码以将其请求超时增加到 5 分钟.
- D. 将报告发布到 Amazon S3, 并使用 Amazon CloudFront 下载到用户.

答案:A

**Q174.** 一家公司决定将其三层 Web 应用程序从本地迁移到 AWS Cloud. 新数据库必须能够动态扩展存储容量并执行表联接.  
哪种 AWS 服务符合这些要求?

- A. 亚马逊极光
- B. 适用于 SqlServer 的 Amazon RDS
- C. Amazon DynamoDB 流
- D. 按需 Amazon DynamoDB

答案:A

**Q175.** 一家公司在 ELB 应用程序负载均衡器后面的 Amazon EC2 实例上运行网站. Amazon Route 53 用于 DNS. 该公司希望建立一个备份网站, 其中包含一条消息, 其中包括主站点关闭时用户可以访问的电话号码和电子邮件地址.  
公司应如何部署此解决方案?

- A. 将 Amazon S3 网站托管用于备份网站和 Route 53 故障转移路由策略.
- B. 将 Amazon S3 网站托管用于备份网站和 Route 53 延迟路由策略.
- C. 在另一个 AWS 区域中部署应用程序, 并使用 ELB 运行状况检查进行故障转移路由.
- D. 在另一个 AWS 区域中部署应用程序, 并在主网站上使用服务器端重定向.

答案:A

**Q176.** 公司需要实现一个关系数据库, 该数据库的多区域灾难恢复恢复点目标 (RPO) 为 1 秒, 恢复时间目标 (RTO) 为 1 分钟.  
哪种 AWS 解决方案可以实现这一目标?

- A. Amazon Aurora 全球数据库
- B. Amazon DynamoDB 全局表.
- C. 启用了多可用区的适用于 MySQL 的 Amazon RDS.
- D. 具有跨区域快照副本的 Amazon RDS for MySQL.

答案:A

**Q177.** 一家运行本地应用程序的公司正在将应用程序迁移到 AWS, 以提高其弹性和可用性. 当前体系结构使用具有大量读取活动的 Microsoft SQL Server 数据库. 该公司希望探索其他数据库选项, 并在需要时迁移数据库引擎. 开发团队每隔 4 个小时对生产数据库进行一次完整复制, 以填充测试数据库. 在此期间, 用户会遇到延迟. 解决方案架构师应该推荐什么作为替代数据库?

- A. 将 Amazon Aurora 与 Multi-AZ Aurora 副本一起使用，并从 mysqldump 恢复测试数据库.
- B. 将 Amazon Aurora 与 Multi-AZ Aurora 副本一起使用，并从 Amazon RDS 还原测试数据库的快照.
- C. 将 Amazon RDS for MySQL 用于多可用区部署并读取副本，并将备用实例用于测试数据库.
- D. 将 Amazon RDS for SQL Server 用于多可用区部署并读取副本，并从 RDS 还原测试数据库的快照.

答案:B

原始答案为 A , 现更正为 B,

Q178. 目前，某公司将对称加密密钥存储在硬件安全模块 (HSM) 中。解决方案架构师必须设计一个解决方案，以将密钥管理迁移到 AWS。解决方案应允许密钥旋转并支持客户提供的密钥的使用。密钥材料应存放在哪里以满足这些要求？

- A. 亚马逊 S3
- B. AWS Secrets Manager
- C. AWS Systems Manager 参数存储
- D. AWS 密钥管理服务 (AWS KMS)

答案:D

原始答案为 B 现在更正为 D,

Q179. 一家公司希望运行混合工作负载以进行数据处理。数据需要由本地应用程序访问，以使用 NFS 协议进行本地数据处理，还必须可以从 AWS 云访问，以进行进一步的分析和批处理。哪种解决方案可以满足这些要求？

- A. 使用 AWS Storage Gateway 文件网关为 AWS 提供文件存储，然后在 AWS Cloud 中对此数据执行分析.
- B. 使用 AWS Storage Gateway 磁带网关将本地数据的备份复制到 AWS，然后在 AWS 云中对此数据执行分析.
- C. 在存储的卷配置中使用 AWS Storage Gateway 卷网关定期对本地数据进行快照，然后将数据复制到 AWS.
- D. 在缓存的卷配置中使用 AWS Storage Gateway 卷网关来备份 AWS 云中的所有本地存储，然后对云中的此数据执行分析.

答案:A

Q180. 公司必须重新评估对 Auto Scaling 组中当前已配置的 Amazon EC2 实例的需求。当前，Auto Scaling 组配置为在两个可用区中最少两个实例，最多四个实例。解决方案架构师检查了 Amazon CloudWatch 指标，发现 EC2 实例的 CPU 利用率始终较低。解决方案架构师应建议什么，在确保应用程序保持容错能力的同时最大化利用率？

- A. 删除一些 EC2 实例以增加其余实例的利用率.
- B. 增加 CPU 利用率较低的实例的 Amazon Elastic Block Store (Amazon EBS) 容量.
- C. 修改 Auto Scaling 组扩展策略，以基于更高的 CPU 利用率指标进行扩展和伸缩.
- D. 创建一个使用较小实例类型的新启动配置。更新现有的 Auto Scaling 组.

答案:D

**Q181.** 公司的网站为用户提供了可下载的历史绩效报告. 该网站需要一种能够扩展以满足全球公司网站需求的解决方案. 该解决方案应具有成本效益, 限制了? 供应 Info 并提供最快的响应时间. 解决方案架构师应推荐哪种组合来满足这些要求?

- A.Amazon CloudFront 和 Amazon S3
- B.AWS Lambda 和 Amazon Dynamo
- C.具有 Amazon EC2 Auto Scaling 的 Application Load Balancer
- D.具有内部应用程序负载平衡的 Amazon Route 53

答案:A

**Q182.** 一家公司正在开发一种实时乘数游戏, 该游戏使用 UDP 在 Auto Scaling 组中的客户端和服务器之间进行通信, 预计白天会有大量需求激增, 因此游戏服务器平台必须相应地进行调整. 开发人员希望将玩家分数和其他非关系数据存储在数据库解决方案中, 该解决方案无需干预即可扩展. 解决方案架构师应建议哪种解决方案?

- A.使用 Amazon Route 53 进行流量分配, 并使用 Amazon Aurora Serverless 进行数据存储.
- B.使用网络负载平衡器进行流量分配, 并按需使用 Amazon DynamoDB 进行数据存储.
- C.使用网络负载平衡器进行流量分配, 并使用 Amazon Aurora Global 进行数据存储.
- D.使用应用程序负载平衡器进行流量分配, 并使用 Amazon DynamoDB 全局表进行数据存储

答案:B

**Q183.** 一家公司目前拥有以供应商专有格式存储在 Amazon S3 中的 250 TB 备份文件. 该公司希望使用供应商提供的基于 Linux 的软件应用程序从 Amazon S3 检索文件, 将文件转换为行业标准格式, 然后将其重新上传到 Amazon S3. 该公司希望最大限度地减少与此对话相关的数据传输费用. 解决方案架构师应该怎么做才能做到这一点?

- A.将转换软件安装为 Amazon S3 批处理操作, 以便在不离开 Amazon S3 的情况下转换数据.
- B.将转换软件安装到本地虚拟机上. 执行转换并将文件从虚拟机重新上传到 Amazon S3.
- C.使用 AWS Snowball Edge 设备对数据进行专家处理并将转换软件安装到设备上. 执行数据转换并将文件从 Snowball 设备重新上传到 Amazon S3.
- D.在与 Amazon S3 相同的区域中启动 Amazon EC2 实例, 然后将转换软件安装到该实例上. 执行转换并将文件从 EC2 实例重新上传到 Amazon S3.

答案:D

**Q184.** 一家公司有一个运行在私有子网中的 Amazon EC2 实例, 该实例需要访问公共网站才能下载补丁程序和更新. 该公司不希望外部网站看到 EC2 实例 IP 地址或与其建立连接. 解决方案架构师如何实现此目标?

- A.在私有子网和部署公共站点的网络之间创建站点到站点 VPN 连接
- B.在公共子网中创建 NAT 网关通过 NAI 网关路由来自私有子网的出站流量
- C.为私有子网创建一个网络 ACL, 其中部署的 EC2 实例仅允许从公共网站的 IP 地址范围进行访问

D. 创建一个仅允许来自公共网站 IP 地址范围的连接的安全组.  
将安全组附加到 EC2 实例.

答案:B

**Q185.** 一家公司已在另一个区域中为其环境创建了隔离备份. 该应用程序在热备份模式下运行, 并且位于应用程序负载平衡器 (ALB) 的前面. 当前的故障转移过程是手动的, 需要更新 DNS 别名记录以指向另一个区域中的辅助 ALB.

解决方案架构师应该怎么做才能使故障转移过程自动化?

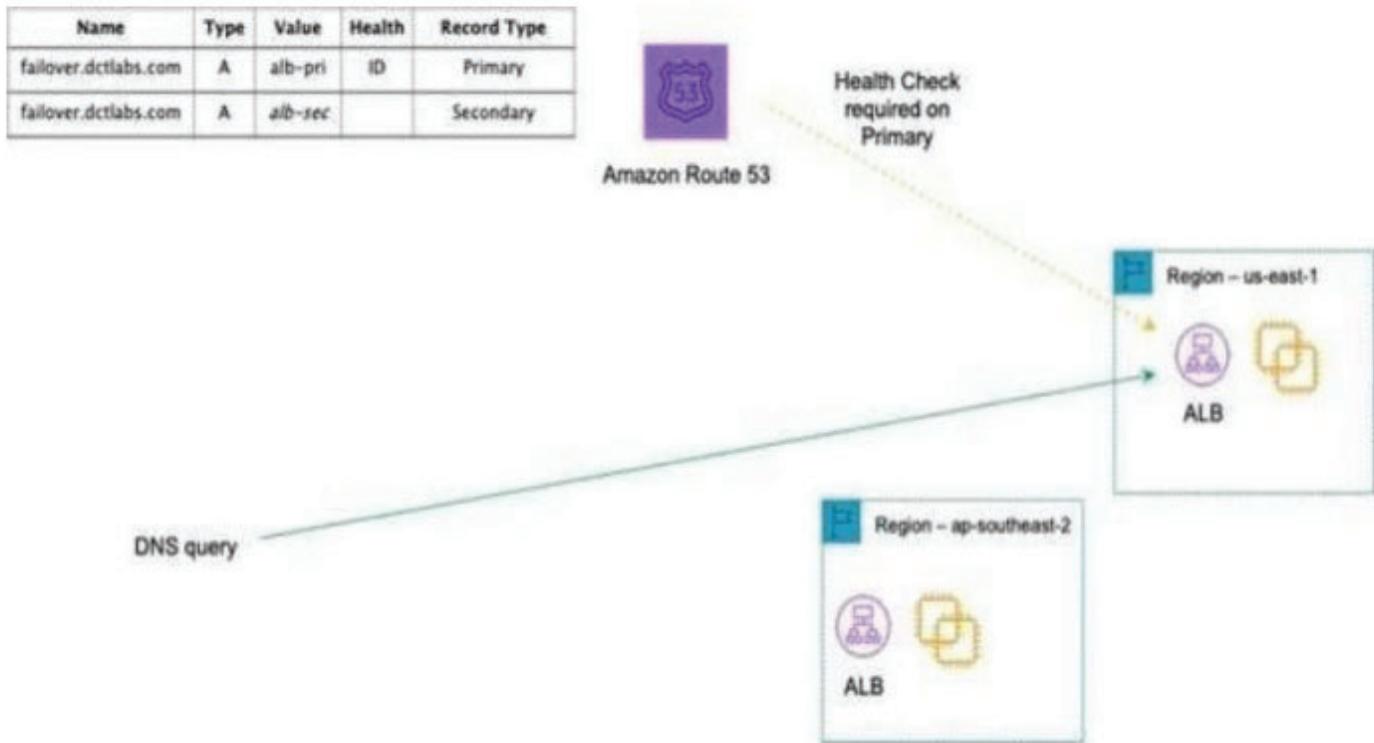
- A. 启用 ALB 健康检查
- B. 启用 Amazon Route 53 健康检查.
- C. 在 Amazon Route 53 上创建一个指向 ALB 端点的 CNAME 记录.
- D. 在指向内部 BIND DNS 服务器的 Amazon Route 53 上创建条件转发规则.

答案:B

您可以使用 Route 53 来检查资源的运行状况, 并且仅返回健康的资源以响应 DNS 查询. DNS 故障转移配置分为三种类型:

1. 主动-被动: 路由 53 主动返回主要资源. 如果发生故障, Route 53 将返回备份资源. 使用故障转移策略进行配置.
2. 主动-主动: 路由 53 主动返回多个资源. 如果发生故障, 路由 53 会故障回复到健康资源. 使用除故障转移以外的任何路由策略进行配置.
3. 组合: 多种路由策略 (例如基于延迟, 加权等) 组合到树中, 以配置更复杂的 DNS 故障转移. 在这种情况下, 辅助 ALB 的别名已经存在. 因此, 解决方案架构师仅需要通过 Amazon Route 53 运行状况检查启用故障转移配置.

配置如下所示:



正确：“启用 Amazon Route 53 健康检查”是正确的答案。错误：“启用 ALB 健康检查”不正确。ALB 健康检查的重点是识别目标（EC2 实例）的健康。它不能将客户端重定向到另一个区域。错误：“在 Amazon Route 53 上创建指向 ALB 端点的 CNAME 记录”不正确，因为别名记录已经存在，并且更适合映射到 ALB。不正确：“在 Amazon Route 53 上创建基于延迟的路由策略”是不正确的，因为这将仅考虑延迟，而未用于故障转移。  
参考文献：

<https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/> 通过我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

**Q186.** 公司需要与外部供应商共享一个 Amazon S3 存储桶。存储桶拥有者必须能够访问所有对象。

应该采取什么行动来共享 S3 存储桶？

- A. 将存储桶更新为请求者付款存储桶
- B. 更新存储桶以启用跨域资源共享（CPORS）
- C. 创建一个存储桶策略，要求用户在上传对象时授予存储桶所有者已满
- D. 创建一个 IAM 策略，要求用户在上载对象时授予存储桶拥有者完全控制权。

答案:C

**Q187.** 一家公司使用 Amazon S3 作为其对象存储解决方案. 该公司有数千个 S3 用于存储数据. 一些 S3 存储桶具有比其他数据访问频率较低的数据. 解决方案架构师发现, 生命周期策略不是始终如一地实施或部分实施. 导致数据存储在高成本的存储中. 哪种解决方案可以在不影响对象可用性的情况下降低成本?

- A. 使用 S3 ACL
- B. 使用 Amazon Elastic Block Store (EBS) 自动快照
- C. 使用 S3 智能分层存储
- D. 使用 S3 一区不频繁访问 (S3 一区-IA).

答案:C

**Q188.** 解决方案架构师正在对最近迁移的工作负载执行安全检查. 工作负载是一个 Web 应用程序, 由 Application Load Balancer 后面的 Auto Scaling 组中的 Amazon EC2 实例组成. 解决方案架构师必须改善安全状况, 并最大程度地减少 DDoS 攻击对资源的影响. 哪种解决方案最有效?

- A. 使用基于速率的规则配置 AWS WAF ACL 创建指向应用程序负载均衡器的 Amazon CloudFront 分配. 在 CloudFront 分布上启用 EAF ACL
- B. 创建一个自定义 AWS Lambda 函数, 该函数将已识别的攻击添加到通用漏洞池中以捕获潜在的 DDoS 攻击. 使用识别的信息来修改网络 ACL 以阻止访问.
- C. 启用 VPC 流日志, 然后将其存储在 Amazon S3 中. 创建自定义 AWS Lambda 函数, 该函数分析日志以查找 DDoS 攻击. 修改网络 ACL 以阻止已标识的源 IP 地址.
- D. 启用 Amazon GuardDuty 并配置写入的结果 10 Amazon CloudWatch 使用 Cloud Watch Events 为触发 Amazon Simple Notification Service (Amazon SNS) 的 DDoS 警报创建事件让 Amazon SNS 调用自定义 AWS Lambda 函数来解析日志以寻找 DDoS 攻击修改网络 ACL 以阻止已标识的源 IP 地址

答案:A

**Q189.** 公司在 Amazon EC2 实例上运行的自定义应用程序具有:

- 从 Amazon S3 读取大量数据
- 执行多阶段分析
- 将结果写入 Amazon DynamoDB

在多阶段分析过程中, 应用程序将写入大量的大型临时文件. 处理性能取决于临时存储性能. 保存临时文件最快的存储方式是什么?

- A. 具有传输加速功能的多个 Amazon S3 存储桶用于存储
- B. 具有预配置 IOPS 和 EBS 优化的多个 Amazon EBS 驱动器
- C. 使用网络托管系统版本 4.1 (NFSv4.1) 协议的多个 Amazon EFS 卷.
- D. 具有软件 RAID 0 的多个实例存储卷.

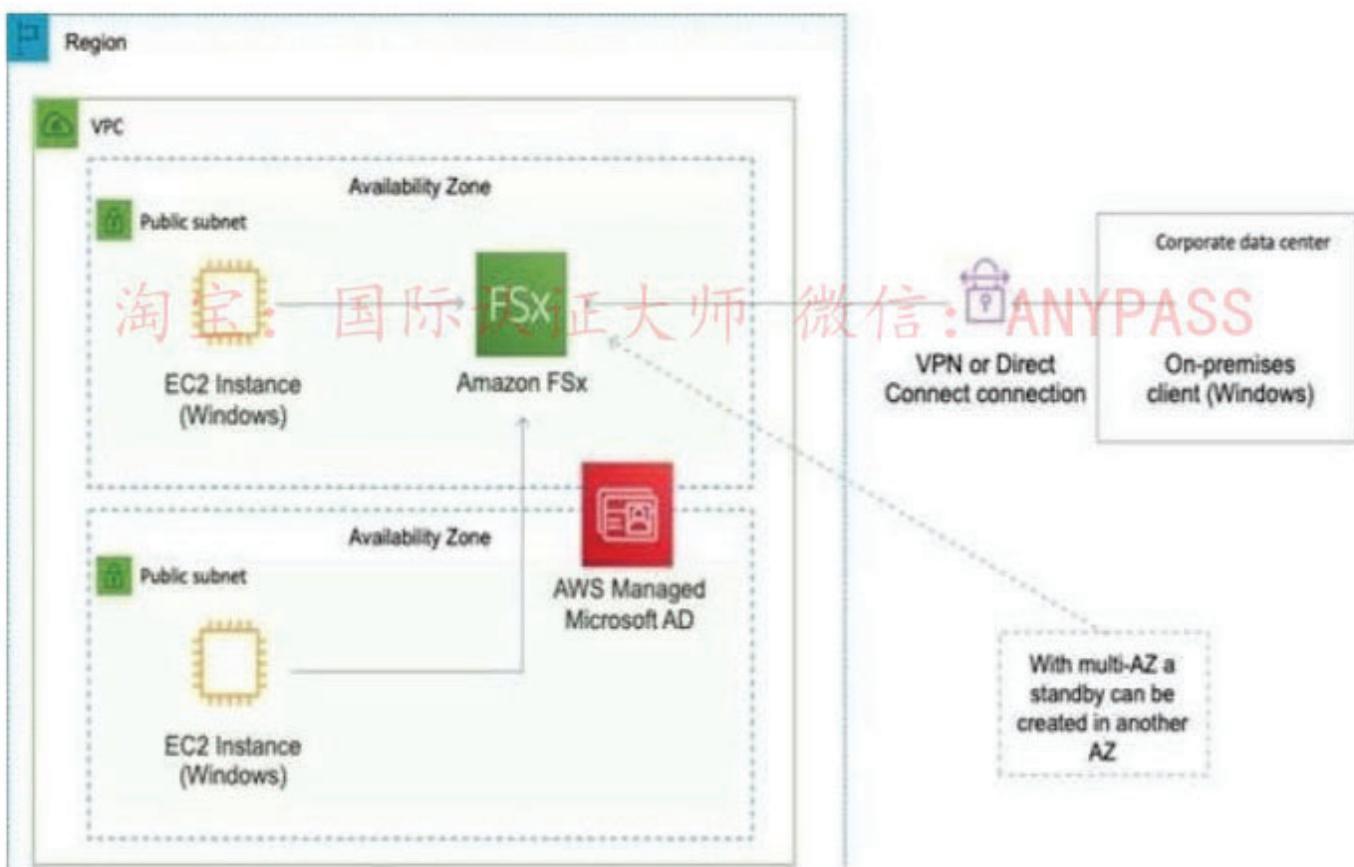
答案:B

Q190. 解决方案架构师必须将 Windows Internet 信息服务 (IIS) Web 应用程序迁移到 AWS. 该应用程序当前依赖于用户的本地网络连接存储 (NAS) 中托管的文件共享. 所设计的解决方案已建议迁移 IIS Web 服务器哪些替代本地 File 共享是最有弹性和持久性的?

- A. 将文件“共享”迁移到 Amazon RDS.
- B. 将磁贴共享迁移到 AWS Storage Gateway
- C. 将文件 Share 迁移到 Amazon FSx or Windows File Server.
- D. 将切片共享迁移到 Amazon Elastic File System (Amazon EFS)

答案:C

适用于 Windows 的 Amazon FSx File Server 提供了完全托管的，高度可靠的文件存储，可通过行业标准的服务器消息块 (SMB) 协议进行访问. 它基于 Windows Server 构建，提供了广泛的管理功能，例如用户配额，最终用户文件还原以及 Microsoft Active Directory (AD) 集成. 它提供了单可用区和多可用区部署选项，完全托管的备份以及静止和传输中的数据加密.



这是提供的唯一为 Windows 实例提供弹性存储的解决方案，正确：“将文件共享迁移到 Windows 文件服务器的 Amazon FSx”是正确的答案.

错误：“无法将文件共享迁移到 Amazon Elastic File System (Amazon EFS)”，因为您无法将 Windows 实例与 Amazon EFS 一起使用.

错误：“将文件共享迁移到 Amazon RDS”不正确，因为这不是用于多可用区部署的共享存储解决方案.

不正确：“将文件共享迁移到 AWS Storage Gateway”不正确，因为 Storage Gateway 复制的文件最终存储在 Amazon S3 上。替代存储解决方案应该是文件共享，而不是基于对象的存储系统。

参考文献：

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

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect- associate / storage / amazon-s3 />

**Q191.** 在 VPC-A 中的 Amazon EC2 实例上运行的应用程序需要访问 VPC-B 中另一个 EC2 实例中的文件。两者是分开的 AWS 账户。网络管理员需要设计一种解决方案，以允许从 VPC-A 安全访问 VPC-B 中的 EC2 实例。

A. 连接不应有单点故障或带宽问题。

哪种解决方案可以满足这些要求？

B. 在 VPC-A 和 VPC-B 之间建立 VPC 对等连接。

C. 为在 VPC-B 中运行的 EC2 实例设置 VPC 网关端点。

D. 将虚拟专用网关连接到 VPC-B 并启用从 VPC-A 进行路由。

E. 为在 VPC-B 中运行的 EC2 实例创建专用虚拟接口（VIF），并从 VPC-B 添加适当的路由。

答案：A

**Q192.** 一家公司看到了一些可疑 IP 地址的访问请求。安全团队发现请求来自相同 CIDR 范围内的不同 IP 地址。解决方案架构师应向团队推荐什么？

A. 在安全性的入站表中添加一条规则，以拒绝来自该 CIDR 范围的流量。

B. 在安全组的出站表中添加一条规则，以拒绝来自该 CIDR 范围的流量。

C. 在网络 ACL 的入站表中添加一个拒绝规则，该规则的编号要比其他规则少。

D. 在网络 ACL 的出站表中添加一个拒绝规则，该规则的规则号比其他规则要少。

答案：C

您只能使用网络 ACL 创建拒绝规则，而使用安全组则无法创建拒绝规则。网络 ACL 从编号最小的规则到编号最高的规则依次处理规则，直到它们到达并允许或拒绝为止。下表描述了安全组和网络 ACL 之间的一些区别：

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

因此，解决方案架构师应在网络 ACL 的入站表中添加一个拒绝规则，该规则的规则编号比其他规则要少。

正确：“在网络 ACL 的入站表中添加一个拒绝规则，其规则号比其他规则要少”是正确的答案。

错误：“在网络 ACL 的出站表中添加一条规则编号比其他规则小的拒绝规则”是错误的，因为这只会阻止出站流量。错误：由于无法使用安全组创建拒绝规则，因此“在安全组的入站表中添加规则以拒绝来自该 CIDR 范围的流量”是错误的。错误：由于您无法使用安全组创建拒绝规则，因此“在安全组的出站表中添加规则以拒绝来自该 CIDR 范围的流量”是错误的。ANYPASS

参考文献：

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html> 使用我们针对考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

**Q193.** 公司正在使用 VPC 对等策略在单个区域中连接其 VPC，以允许交叉通信。最近帐户创建和 VPC 的增加使维持 VPC 对等策略变得困难，该公司预计将增长到数百个 VPC。还提出了一些使用某些 VPC 创建站点到站点 VPN 的新请求。解决方案架构师的任务是为多个帐户，VPNS 和 VPN 创建集中式网络设置。

哪种网络解决方案满足这些要求？

- A. 配置共享的 VPC 和 VPN 并互相共享
- B. 配置中心辐射型，并通过 VPC 对等路由所有流量。
- C. 在所有 VPC 和 VPN 之间配置一个 AWS Direct Connect。
- D. 使用 AWS Transit Gateway 配置一个传输网关，并连接所有 VPC 和 VPN。

答案:D

**Q194.** 整体应用程序最近已迁移到 AWS，现在正在单个 Amazon EC2 实例上运行。由于应用程序的限制，不可能使用自动缩放来扩展应用程序。首席技术官（CTO）希望自动化解决方案在基础硬件出现故障的不太可能的情况下还原 EC2 实例。如何使 EC2 实例尽快自动恢复？

- A. 配置一个 Amazon CloudWatch 警报，如果警报受损，该警报将触发 EC2 实例的恢复。
- B. 配置 Amazon CloudWatch 警报以触发 SNS 消息，以便在 EC2 实例受损时向 CTO 发出警报。
- C. 配置 AWS CloudTrail 来监视 EC2 实例的运行状况，如果它受损，则触发实例恢复。
- D. 配置一个 Amazon EventBridge 事件以每小时一次触发一次 AWS Lambda 函数，该函数检查 EC2 实例的运行状况，并在 EC2 实例运行不正常时触发实例恢复。

答案:A

原始答案为 B，现更正为 A。

**Q195.** 一家公司创建了一个 VPC，该 VPC 在多个可用区（AZ）中具有多个专用子网，在一个可用区中具有一个公共子网。公共子网用于启动 NAT 网关。专用子网中有使用 NAT 网关连接到 Internet 的实例。如果使用了 AZ 故障，该公司希望确保该实例并非都遇到 Internet 连接问题，并且要准备好备份计划。解决方案架构师应建议哪种解决方案具有最高的可用性？

- A. 在同一个可用区中使用 NAT 网关创建一个新的公共子网在两个 NAT 网关之间分配流量
- B. 在现在的公共子网中创建一个 Amazon EC2 NAT 实例在 NAT 网关和 NAT 实例之间分配流量
- C. 在每个 AZ 中创建公共子网，并在每个子网中启动 NAT 网关配置从每个 AZ 中的私有子网到相应 NAT 网关的流量
- D. 在同一公共子网中创建 Amazon EC2 NAT 实例将 NAT 网关替换为 NAT 实例，并将该实例与具有适当扩展策略的 Auto Scaling 组相关联。

答案:C 淘宝：国际认证大师 微信：ANYPASS

**Q196.** 一家公司有多个适用于各个部门的 AWS 账户。其中一个部门希望与所有其他部门共享一个 Amazon S3 存储桶。哪种解决方案需要最少的努力？

- A. 为存储桶启用跨帐户 S3 复制
- B. 创建一个预签名的 URL 来存储桶并与其他部门共享
- C. 设置 S3 存储桶策略以允许跨帐户访问其他部门
- D. 为每个部门创建 IAM 用户并配置一个只读 IAM 策略

答案:C

**Q197.** 一家公司收集多个大洲城市的温度、湿度和大气压力数据。每个站点每天收集的平均数据量为 500 GB。每个站点都有高速互联网连接。该公司的天气预报应用程序位于单个区域中，并每天分析数据。

汇总所有这些全球站点的数据的最快方法是什么？

- A. 在目标存储桶上启用 **Amazon S3 Transfer Acceleration** 使用分段上传将网站数据直接上传到目标存储桶。
- B. 将站点数据上传到最近的 AWS 区域中的 Amazon S3 存储桶。使用 S3 跨区域复制将对象复制到目标存储桶。

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- C. 将站点数据上传到最近的 AWS 区域中的 Amazon S3 存储桶。使用 S3 跨区域复制将对象复制到目标存储桶。
- D. 将数据上传到关闭区域中的 Amazon EC2 实例。将数据存储在 Amazon EBS 卷中。每天拍摄一张 EBS 快照并将其复制到集中区域。恢复集中区域中的 EBS 卷，并每天对数据进行分析。

答案:A

Q198. 一家公司已在 AWS Lambda 上实现了其微服务之一，该微服务访问了名为 Books 的 Amazon DynamoDB 表。解决方案架构师正在设计一个 IAM 策略，该策略将附加到 Lambda 函数的 IAM 角色，从而使其可以访问，更新和删除 Books 表中的项目。IAM 策略必须阻止功能对“书籍”表或任何其他操作执行任何其他操作。哪种 IAM 策略可以满足这些需求并提供最小的特权访问？

一个)

```
{  
    "Version" : "2012-10-17" ,  
    "Statement" : [  
        {  
            "Sid" :" PutUpdateDeleteOnBooks" ,  
            "Effect" :" Allow" ,  
            "Action": "Dynamodb:PutItem" ,  
            "Dynamodb:UpdateItem" ,  
            "Dynamodb:DeleteItem"  
        },  
        {"Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/Books"  
    }  
]
```

B)

```
{  
    "Version" : "2012-10-17" ,  
    "Statement" : [  
        {  
            "Sid" :" PutUpdateDeleteOnBooks" ,  
            "Effect" :" Allow" ,  
            "Action" : [  
                "Dynamodb:PutItem" ,  
                "Dynamodb:UpdateItem" ,  
                "Dynamodb:DeleteItem"  
            ],  
            "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/* "  
        }  
    ]  
}
```

淘宝：国际认证大师 微信：ANYPASS

c)

```
{  
    "Version" : "2012-10-17" ,  
    "Statement" : [  
        {  
            "Sid" :" PutUpdateDeleteOnBooks" ,  
            "Effect" :" Allow" ,  
            "Action" : "Dynamodb:*" ,  
            "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/Books "  
        }  
    ]  
}
```

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

D)

```
{  
    "Version" : "2012-10-17" ,  
    "Statement" : [  
        {  
            "Sid" :" PutUpdateDeleteOnBooks" ,  
            "Effect" :" Allow" ,  
            "Action" : "Dynamodb:*" ,  
            "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/Books"  
        },  
        {  
            "Sid" :" PutUpdateDeleteOnBooks" ,  
            "Effect" :" Deny" ,  
            "Action" : "Dynamodb:*" ,  
            "Resource" :" arn:aws:dynamodb:us-west-2:123456789012:table/Books"  
        }  
    ]  
}
```

- A.选项 A
- B.方案 B
- C.方案 C
- D.选项 D

答案:A

Q199. 应用程序开发人员已经注意到,当业务报告用户针对支持该应用程序的 Amazon RDS 实例运行大型生产报告时,生产应用程序非常慢. 报告查询运行时, RDS 实例-d 的 CPU 和内存利用率指标不超过 60%. 业务报告用户必须能够生成报告,而不影响应用程序性能.  
哪个动作可以完成此任务?

- A.增加 RDS 实例的大小
- B.创建一个只读副本并将应用程序连接到它.
- C.在 RDS 实例上启用多个可用区

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

D. 创建一个只读复制并将业务报告连接到该复制.

答案:D

**Q200.** 公司的打包应用程序可以动态创建并返回一次性文本文件, 以响应用户请求. 该公司正在使用 Amazon CloudFront 进行分发, 但希望将来减少数据传输成本. 该公司修改了应用程序的源代码.

解决方案架构师应该怎么做才能降低成本?

- A. 使用 Lambda 格言在将文件发送给用户时对其进行压缩.
- B. 启用 Amazon S3 Transfer Acceleration 以减少响应时间.
- C. 在 CloudFront 分布上启用缓存以将生成的文件存储在边缘.
- D. 使用 Amazon S3 分段上传将文件移至 Amazon S3, 然后再将其返回给用户.

答案:C

**Q201.** 面向公众的 Web 应用程序查询专用子网中 Amazon EC2 实例上托管的数据库. 大量查询涉及多个表联接, 并且由于复杂查询的增加, 应用程序性能一直在下降. 应用程序团队将执行更新以提高性能.

解决方案架构师应向应用程序团队推荐什么? (选择两个.)

- A. 在 Amazon SQS 中缓存查询数据
- B. 创建一个只读副本以减轻查询负担
- C. 将数据库迁移到 **Amazon Athena**
- D. 实施 Amazon DynamoDB Accelerator 以缓存数据.
- E. 将数据库迁移到 Amazon RDS

答案:BE

**Q202.** 公司有一个基于 Microsoft Windows 的应用程序, 必须将其迁移到 AWS. 此应用程序需要使用附加到多个 Amazon EC2 Windows 实例的共享 Windows 文件系统. 解决方案架构师应该怎么做才能做到这一点?

- A. 使用 Amazon EFS 配置卷将 EPS 卷安装到每个 Windows 实例
- B. 在卷网关模式下配置 AWS Storage Gateway 将卷安装到每个 Windows 实例
- C. 为 Windows 文件服务器配置 Amazon FSx 将 Amazon FSx 卷安装到每个 Windows 实例
- D. 配置具有所需大小的 Amazon EBS 卷将每个 EC2 实例连接到该卷将该卷中的文件系统安装到每个 Windows 实例

答案:C

**Q203.** 一家公司最近在全球扩张, 希望使这些地区的用户可以访问其应用程序. 该应用程序将部署在 Auto Scaling 组中应用程序负载均衡器后面的 Amazon EC2 实例上. 公司需要将流量从一个地区的资源转移到另一个地区的能力.

解决方案架构师应该建议什么?

- A.配置 Amazon Route 53 延迟路由策略
- B.配置 Amazon Route 53 地理位置路由策略
- C.配置 Amazon Route 53 地理邻近结垢策略.
- D.配置 Amazon Route 53 多值答案路由策略

答案:C

原始答案为 B , 现更正为 C

**Q204.** 公司有多个业务系统, 这些业务系统需要访问文件共享中存储的数据. 业务系统将使用服务器消息块 (SMB) 协议访问文件共享. 该文件共享解决方案应该可以从公司的旧式本地环境和 AWS 中进行访问. 哪些服务改变了业务需求? (选择两个. )

- A.亚马逊 EBS
- B.亚马逊 EFS
- C.适用于 Windows 的 Amazon FSx
- D.亚马逊 S3
- E.AWS Storage Gateway 文件网关

答案:CE

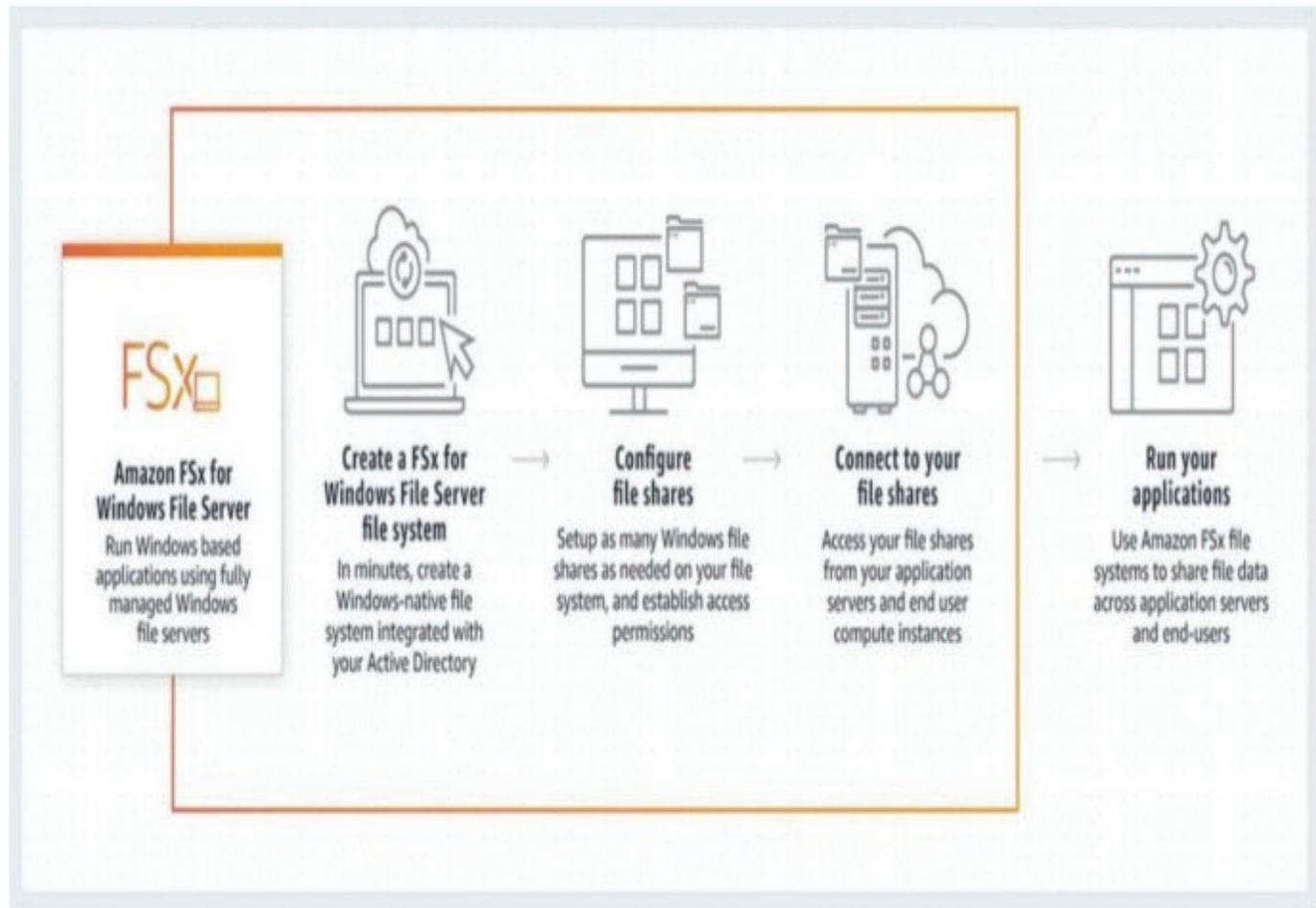
关键字: SMB +本地

条件: 可从本地和 AWS 访问文件

适用于 Windows 文件服务器的 Amazon FSx 微信: ANYPASS

适用于 Windows 的 Amazon FSx File Server 提供了完全托管的, 高度可靠的和可扩展的文件存储, 可以通过行业标准的服务器消息块 (SMB) 协议进行访问. 它基于 Windows Server 构建, 提供了广泛的管理功能, 例如用户配额, 最终用户文件还原以及 Microsoft Active Directory (AD) 集成. 它提供了单可用区和多可用区部署选项, 完全托管的备份以及静态数据和传输数据的加密. 您可以通过 SSD 和 HDD 存储选件来优化成本和性能, 以满足工作负载的需求. 您可以随时扩展存储并更改文件系统的吞吐量性能. 可从 Windows, Linux 和 MacOS 计算实例以及在 AWS 或本地运行的设备访问 Amazon FSx 文件存储.

FSx for Windows File Server 的工作方式



淘宝：国际认证大师 微信：ANYPASS  
AWS 存储网关

AWS Storage Gateway 是一种混合云存储服务，可让您在内部访问几乎无限的云存储。客户使用 Storage Gateway 简化了存储管理并降低了关键混合云存储用例的成本。这些措施包括将备份移至云，使用由云存储支持的本地文件共享，以及为本地应用程序提供对 AWS 中数据的低延迟访问。

## 文件

为了支持这些用例，Storage Gateway 提供了三种不同类型的网关？它们可以无缝地连接内部部署

网关，磁带网关和卷网关

应用程序到云存储，在本地缓存数据以实现低延迟访问。您的应用程序使用标准存储协议（例如 NFS, SMB 和 iSCSI）通过虚拟机或网关硬件设备连接到服务。网关连接到 AWS 存储服务，例如 Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS 和 AWS Backup，为 AWS 中的文件，卷，快照和虚拟磁带提供存储。该服务包括高度优化和高效的数据传输机制，具有带宽管理和自动网络弹性。

## Storage Gateway 的工作方式



下表显示了可用的不同网关以及接口和用例：

New Name	Old Name	Interface	Use Case
File Gateway	None	NFS, SMB	Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount points
Volume Gateway Stored Mode	Gateway-Stored Volumes	iSCSI	Asynchronous replication of on-prem data to S3
Volume Gateway Cached Mode	Gateway-Cached Volumes	iSCSI	Primary data stored in S3 with frequently accessed data cached locally on-prem
Tape Gateway	Gateway-Virtual Tape Library	iSCSI	Virtual media changer and tape library for use with existing backup software

正确：“适用于 Windows 的 Amazon FSx”是正确的答案。正确：“Amazon Storage File Gateway”是正确的答案。

错误：“Amazon EBS”不正确，因为不支持 NFS / SMB。错误：“Amazon EFS”不正确，因为不支持 NFS / SMB。错误：“Amazon S3”不正确，因为不支持 NFS / SMB。

参考文献：

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

<https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

<https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/>

<https://d0.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf>

<https://youtu.be/T5KlnNj7-qg>

使用我们特定于考试的备忘单节省时间：

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

**Q205.** 公司的运营团队已将现有的 Amazon S3 存储桶配置为在存储桶中创建新对象时通知 Amazon SQS 队列。开发团队还希望在创建新对象时接收事件。现有的运营团队工作流程必须保持不变。

哪种解决方案可以满足这些要求？

- A. 创建另一个 SQS 队列更新存储桶中的 S3 事件，以便在创建新对象时也更新新队列。
- B. 创建一个仅允许 Amazon S3 访问该队列的新 SQS 队列，在创建新对象时，Update Amazon S3 更新此队列
- C. 为更新创建一个 Amazon SNS 主题和 SQS 队列。更新存储桶以将事件发送到新主题。更新两个队列以轮询 Amazon SNS。
- D. 为存储桶更新创建一个 Amazon SNS 主题和 SQS 队列。更新存储桶以将事件发送到新主题，为主题中的两个队列添加订阅。

答案:D

**Q206.** 一家公司希望为其在 Windows Server 2016 上的 Amazon EC2 实例上运行的.NET 应用程序服务器和 Microsoft SQL Server 数据库部署共享文件系统。该解决方案必须能够集成到公司 Active Directory 域中，并且必须高度耐用，由 AWS 管理，并提供吞吐量和 IOPS 级别。

哪种解决方案满足这些要求？

- A. 将 Amazon FSx 用于 Windows 文件服务器
- B. 使用 Amazon Elastic File System (Amazon EFS)
- C. 在文件网关模式下使用 AWS Storage Gateway.
- D. 在两个可用区中的两个点播实例上部署 Windows 文件服务器。

答案:A

**Q207.** 一家公司正在设计一项新服务，该服务将在 Elastic Load Balancer 后面的 Amazon EC2 实例上运行。但是，许多 Web 服务客户端只能访问其防火墙上列入白名单的 IP 地址。

解决方案架构师应建议什么来满足客户的需求？解决方案架构师应建议什么来满足客户的需求？

- A. 具有关联的弹性 IP 地址的网络负载平衡器。
- B. 具有关联的弹性 IP 地址的 Application Load Balancer
- C. Amazon Route 53 托管区域中的 A 记录指向弹性 IP 地址
- D. 一个 EC2 实例，其公共 IP 地址在负载均衡器之前作为代理运行

答案:A

**Q208.** 一家公司正在设计一项新服务，该服务将在 Elastic Load Balancer 后面的 Amazon EC2 实例上运行。

但是，许多 Web 服务客户端只能访问其防火墙上列入白名单的 IP 地址。

解决方案架构师应建议什么来满足客户的需求？

- A. 具有关联的弹性 IP 地址的网络负载平衡器。
- B. 具有关联的弹性 IP 地址的 Application Load Balancer
- C. Amazon Route 53 托管区域中的 A 记录指向弹性 IP 地址

D.一个 EC2 实例，其公共 IP 地址在负载均衡器之前作为代理运行

答案:A

**Q209.** 一家公司正在研究潜在的解决方案，这些解决方案将收集，处理和存储用户的服务使用数据。

业务目标是创建一种分析功能，使公司能够使用标准 SQL 查询快速收集运营见解。该解决方案应具有高可用性，并确保数据层中的原子性，一致性，隔离性和耐用性（ACID）合规性。

解决方案架构师应建议哪种解决方案？

- A. 使用 Amazon DynamoDB 交易
- B. 在多可用区设计中创建 Amazon Neptune 数据库
- C. 在多可用区设计中为 MySQL 数据库使用完全托管的 Amazon RDS
- D. 在使用 Amazon EBS 吞吐量优化 HDD (st1) 存储的 Amazon EC2 实例上部署 PostgreSQL.

答案:C

原始答案 A，现在更正为 C，

**Q210.** 一家公司在 Application Load Balancer 后面的 Amazon CC2 实例上运行 Web 服务。实例在两个可用区中的 Amazon EC2 Auto Scaling 组中运行。该公司需要最少的巡回实例 a！所有石灰满足所需的服务水平协议（SLA），同时保持较低的成本。

如果可用区不足，公司如何保持与 SLA 的合规性？

- A. 添加目标跟踪缩放策略且冷却时间很短
- B. 更改 Auto Scaling 组启动配置以使用更大的实例类型
- C. 更改 Auto Scaling 组以在三个可用区中使用六台服务器
- D. 更改 Auto Scaling 组以在两个可用区中使用八台服务器

答案:A

**Q211.** 一家电子商务公司注意到其基于 Amazon RDS 的 Web 应用程序的性能下降。

性能下降归因于业务分析师触发的只读 SQL 查询数量的增加。

解决方案架构师需要以对现有 Web 应用程序的最小更改来解决问题。

解决方案架构师应该建议什么？

- A. 将数据导出到 Amazon DynamoDB，并让业务分析师运行其查询。
- B. 将数据加载到 Amazon ElasticCache 中，并让业务分析师运行其查询。
- C. 创建主数据库的只读副本，并让业务分析师运行其查询。
- D. 将数据复制到 Amazon Redshift 集群中，并让业务分析师运行其查询。

答案:C

**Q212.** 一家公司正在容器中构建应用程序。

该公司希望将其本地开发和运营服务从其内部数据中心迁移到 AWS。

管理层指出，生产系统必须与云无关，并且在整个生产系统中使用相同的配置和管理员工具。解决方案架构师需要设计一个可与开源软件保持一致的托管解决方案。

哪种解决方案满足这些要求？

- A. 在具有 EC2 实例工作程序节点的 Amazon EC2 上启动容器.
- B. 在 Amazon Elastic Kubernetes Service (Amazon EKS) 和 EKS worker 节点上启动容器.
- C. 使用 AWS Fargate 实例在 Amazon Elastic Containers 服务 (Amazon ECS) 上启动容器.
- D. 使用 Amazon EC2 实例工作程序节点在 Amazon Elastic Container Service (Amazon EC) 上启动容器.

答案:B

Q213. 一家公司正在使用服务运行一个两层电子商务网站. 当前的架构师使用面向发布的 Elastic Load Balancer, 该流量将流量发送到私有子网中的 Amazon EC2 实例.

静态内容托管在 EC2 实例上, 动态内容从 MySQL 数据库检索.

该应用程序正在美国运行. 该公司最近开始向欧洲和澳大利亚的用户销售产品.

解决方案架构师需要设计解决方案, 以便其国际用户拥有更好的浏览体验.

哪种解决方案最划算?

- A. 将整个网站托管在 Amazon S3 上.
- B. 使用 Amazon CloudFront 和 Amazon S3 托管静态图像.
- C. 增加公共负载均衡器和 EC2 实例的数量
- D. 在欧洲和澳大利亚的 AWS 区域中部署两层网站.

答案:B

Q214. 数据库位于经历高度动态读取的 Amazon RDS MySQL 5.6 Multi-AZ 数据库实例上.

在测试辅助 AWS 区域的读取性能时, 应用程序开发人员会注意到速度明显下降.

开发人员需要一种提供少于 1 秒的读取复制延迟的解决方案.

解决方案架构师应该建议什么?

- A. 在二级区域的 Amazon EC2 上安装 MySQL.
- B. 使用跨区域副本将数据库迁移到 Amazon Aurora.
- C. 在辅助数据库中为 MySQL 只读副本创建另一个 RDS.
- D. 实施 Amazon ElastiCache 以提高数据库查询性能.

答案:B

Q215. 运营团队的标准规定, IAM 策略不应直接应用于用户.

一些新成员尚未遵循此标准. 运营经理需要一种方法来轻松识别带有附加策略的用户. 解决方案架构师应该怎么做才能做到这一点?

- A. 使用 AWS CloudTrail 进行监控
- B. 创建一个 AWS Config 规则以每天运行
- C. 在 Amazon SNS 上发布 IAM 用户更改
- D. 修改用户后运行 AWS Lambda

答案:B

**Q216** 一家公司已经建立了一个新的 AWS 账户。该帐户是新设置的，并且未更改默认设置。该公司担心 AWS 账户根用户的安全性。应该采取什么措施来保护 root 用户？

- A. 创建 IAM 用户来执行日常管理任务。  
禁用 root 用户。
- B. 创建 IAM 用户来执行日常管理任务。  
在 root 用户上启用多因素身份验证。
- C. 为根用户生成访问密钥。  
将访问密钥（而不是 AWS 管理控制台）用于日常管理任务。
- D. 向最高级的解决方案架构师提供 root 用户凭据。  
让解决方案架构师使用 root 用户执行日常管理任务。

答案:B

原始答案为 D，现更正为 B，

**Q217.** 一家医疗保健公司存储高度敏感的患者记录。合规性要求将多份副本存储在不同的位置。每条记录必须存储 7 年。该公司拥有服务水平协议（SLA），可以在前 30 天立即向政府机构提供记录，然后在请求后的 4 小时内提供记录。解决方案架构师应该建议什么？

- A. 在启用跨区域复制的情况下使用 Amazon S3。  
30 天后，使用生命周期策略将数据过渡到 Amazon S3 Glacier
- B. 在启用跨域资源共享（CORS）的情况下使用 Amazon S3。  
30 天后，使用生命周期策略将数据过渡到 Amazon S3 Glacier.
- C. 在启用跨区域复制的情况下使用 Amazon S3。  
30 天后，使用生命周期策略将数据过渡到 Amazon S3 Glacier Deep Archive
- D. 在启用跨域资源共享（GORS）的情况下使用 Amazon S3。  
30 天后，使用生命周期策略将数据过渡到 Amazon S3 Glacier Deep Archive

答案:A

**Q218** 解决方案架构师必须创建高度可用的堡垒主机体系结构。该解决方案需要在单个 AWS 区域内具有弹性，并且只需很少的维护工作即可。解决方案架构师应怎么做才能满足这些要求？

- A. 创建一个网络负载均衡器，该负载均衡器由具有 UDP 倾听器的 Auto Scaling 组支持。
- B. 创建一个由 Spot Fleet 支持的网络负载均衡器，该实例具有一个组中的实例以及一个分区放置组中的实例。
- C. 创建一个由不同服务区中的现有服务支持的网络负载平衡器作为目标。
- D. 创建一个由 Auto Scaling 支持的网络负载均衡器，并以多个可用区中的实例为目标

答案:D

**Q219.** 解决方案架构师正在使用 AWS 云设计混合应用程序。内部数据中心与 AWS 之间的网络将使用 AWS Direct Connect (DX) 连接。

AWS 与本地数据中心之间的应用程序连接必须具有高度的弹性。

应该实现哪种 DX 配置以满足这些要求？

- A. 在 DX 连接上配置一个 VPN.
- B. 在多个 DX 位置配置 DX 连接.
- C. 使用最可靠的 DX 伙伴配置 DX 连接.
- D. 在 DX 连接的顶部配置多个虚拟接口.

答案:B

**Q220.** 一家公司计划在 Amazon S3 上存储敏感用户数据。内部安全合规性要求先将数据加密，然后再将数据发送到 Amazon S3。

解决方案架构师应建议哪些以满足这些要求？

- A. 使用客户提供的加密密钥进行服务器端加密
- B. 使用 Amazon S3 托管加密密钥进行客户端加密
- C. 使用存储在 AWS Key Management Service (AWS KMS) 中的密钥进行服务器端加密
- D. 使用存储在 AWS Key Management Service (AWS KMS) 中的主密钥进行客户端加密

答案:D

**Q221.** 一家公司正在使用 Amazon EC2 来运行其大数据分析工作负载。这些可变的工作负载每天晚上运行，至关重要的是它们要在第二天开始营业时完成。

解决方案架构师的任务是设计成本最低的 MOST 解决方案。

哪种解决方案可以做到这一点？

- A. 现货舰队
- B. 竞价型实例
- C. 预留实例
- D. 按需实例

答案:A

**Q222.** 公司强制要求 Amazon S3 网关终端节点必须仅允许对可信存储桶的流量。

解决方案架构师应采用哪种方法来满足此要求？

- A. 为公司的每个受信任的 S3 存储桶创建一个存储桶策略，该策略仅允许来自公司的受信任 VPC 的流量
- B. 为公司的每个受信任的 S3 存储桶创建一个存储桶策略，该策略仅允许来自公司 S3 网关端点 ID 的流量
- C. 为公司的每个 S3 网关端点创建一个 S3 端点策略，该策略将阻止从除公司的受信任 VPC 之外的任何 VPC 进行访问
- D. 为公司的每个 S3 网关端点创建一个 S3 端点策略，该策略提供对受信任 S3 存储桶的 Amazon 资源名称 (ARN) 的访问

答案:D

**Q223.** 一家公司正在使用 AWS 设计可处理保险报价的 Web 应用程序，用户将向该应用程序请求报价。

报价必须按报价类型分开，必须在 24 小时内回复，并且不得丢失。

该解决方案应该易于设置和维护。

哪种解决方案满足这些要求？

A.根据报价类型创建多个 Amazon Kinesis 数据流。

配置 Web 应用程序以将消息发送到正确的数据流。

配置每个后端应用程序服务器组，以使用 Kinesis Client Library (KCL) 从其自己的数据流中收集消息

B.创建多个 Amazon Simple Notification Service(Amazon SNS)主题，并根据报价类型将 Amazon SQS 队列注册到自己的 SNS 主题。

配置 Web 应用程序以将消息发布到 SNS 主题队列。

配置每个后端应用程序服务器以工作自己的 SQS 队列

C.创建一个单一的 Amazon Simple Notification Service (Amazon SNS) 主题，并将 Amazon SQS 队列订阅到 SNS 主题。

配置 SNS 消息过滤 以根据报价类型将消息发布到正确的 SQS 队列。

配置每个后端应用程序服务器以工作自己的 SQS 队列。

D.根据报价类型创建多个 Amazon Kinesis Data Firehose 交付流，以将数据流交付到 Amazon Elasticsearch Service (Amazon ES) 集群。

配置 Web 应用程序以将消息发送到正确的传递流。

配置应用程序服务器的每个后端组以搜索来自 Amazon ES 的消息并进行相应处理

答案:C

**Q224.** 一家公司在以 Amazon RDS 数据库为后盾的 Amazon EC2 上运行高度敏感的应用程序。

法规要求所有静态身份信息都必须加密。

解决方案架构师应建议哪种解决方案，以最少的基础架构更改来满足此要求"

A.部署 AWS Certificate Manager 以生成证书。

使用证书加密数据库卷

B.部署 AWS CloudHSM. 生成加密密钥，并使用客户主密钥 (CMK) 加密数据库卷。

C.使用 AWS Key Management Service 客户主密钥 (AWS KMS CMK) 配置 SSL 加密以加密数据库卷

D.使用 AWS Key Management Service (AWS KMS) 密钥配置 Amazon Elastic Block Store (Amazon EBS) 加密和 Amazon RDS 加密，以加密实例和数据库卷。

答案:D

**Q225.** 一家公司正在为移动应用程序创建一种架构，该架构需要为其用户提供最小的延迟。该公司的架构由在 Auto Scaling 组中运行的 Application Load Balancer 后面的 Amazon EC2 实例组成。EC2 实例连接到 Amazon RDS. 应用程序 Beta 测试表明，读取数据时速度变慢。但是这些指标表明 EC2 实例未超过任何 CPU 使用率阈值

如何解决这个问题 1?

- A.降低 Auto Scaling 组中 CPU 利用率的阈值
- B.用网络负载平衡器替换应用程序负载平衡器.
- C.为 RDS 实例添加只读副本，并将只读流量定向到该副本.
- D.向 RDS 实例添加多可用区支持，并将读取流量定向到新的 EC2 实例.

答案:C

Q226. 一家公司最近发布了一种新型的互联网传感器. 该公司预计将出售成千上万个传感器，这些传感器旨在将每秒的大量数据流传输到一个中心位置.

解决方案架构师必须设计一种可以吸收和存储数据的解决方案，以便工程团队可以毫秒级的响应速度实时分析数据. 解决方案架构师应建议哪种解决方案？

- A.使用 Amazon SQS 队列提取数据.  
使用 AWS Lambda 函数使用数据，该函数随后将数据存储在 Amazon Redshift 中.
- B.使用 Amazon SOS 队列提取数据.  
使用 AWS Lambda 函数使用数据，该函数随后将数据存储在 Amazon DynamoDB 中.
- C.使用 Amazon Kinesis Data Streams 摄取数据.  
使用 AWS Lambda 函数使用数据，该函数随后将数据存储在 Amazon Redshift 中.
- D.使用 Amazon Kinesis Data Streams 摄取数据.  
使用 AWS Lambda 函数使用数据，该函数随后将数据存储在 Amazon DynamoDB 中.

答案:D

淘宝：国际认证大师 微信：ANYPASS

Q227. 一家公司正在将 NoSQL 数据库集群迁移到 Amazon EC2. 数据库自动复制数据以维护至少三个数据副本. 服务器的 I/O 吞吐量是最高优先级.

解决方案架构师应为迁移建议哪种实例类型？

- A.具有实例存储的存储优化实例
- B.具有 Amazon Elastic Block Store (Amazon EBS) 卷的可突发通用实例
- C.启用 Amazon Elastic Block Store (Amazon EBS) 优化的内存优化实例
- D.在启用 Amazon Elastic Block Store (Amazon EBS) 优化的情况下计算优化实例

答案:A

Q228. 一家公司在 Amazon EC2 Linux 实例上运营一个网站. 某些实例的故障排除指出故障实例上的交换空间不足.

运营团队负责人需要一个解决方案来监控此情况.

解决方案架构师应该建议什么？

- A.配置 Amazon CloudWatch SwapUsage 指标维度.  
在 CloudWatch 的 EC2 指标中监控 SwapUsage 维度.
- B.使用 EC2 元数据收集信息，然后将其发布到 Amazon CloudWatch 自定义指标.  
在 CloudWatch 中监控 SwapUsage 指标.
- C.在实例上安装 Amazon CloudWatch 代理.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- 按照设定的时间表运行适当的脚本.  
在 CloudWatch 中监控 SwapUtilization 指标.  
D. 在 EC2 控制台中启用详细监视.  
创建一个 Amazon CloudWatch SwapUtilization 自定义指标.  
在 CloudWatch 中监控 SwapUtilization 指标.

答案:C

Q229. 公司有两个要迁移到 AWS 的应用程序. 这两个应用程序通过同时访问相同的文件来处理大量文件. 这两个应用程序都需要读取低延迟的文件. 解决方案架构师应针对这种情况推荐哪种架构?

- A. 配置两个 AWS Lambda 函数以运行应用程序.  
使用实例存储卷创建一个 Amazon EC2 实例以存储数据.  
B. 配置两个 AWS Lambda 函数以运行应用程序.  
使用 Amazon Elastic Block Store (Amazon EBS) 卷创建一个 Amazon EC2 实例以存储数据.  
C. 配置一个内存优化的 Amazon EC2 实例以同时运行两个应用程序.  
使用预置的 IOPS 创建 Amazon Elastic Block Store (Amazon EBS) 卷以存储数据.  
D. 配置两个 Amazon EC2 实例以运行两个应用程序.  
使用通用性能模式和突发功能配置 Amazon Elastic File System (Amazon EFS).  
吞吐量模式下存储数据.

答案:D

Q230. 一家公司最近部署了新的审核系统, 以集中有关 Amazon EC2 实例的操作系统版本, 修补程序和已安装软件的信息. 解决方案架构师必须确保通过 EC2 Auto Scaling 组配置的所有实例在启动和终止后立即将其成功发送到审计系统. 哪种解决方案可以最有效地实现这些目标?

- A. 使用预定的 AWS Lambda 函数并在所有 EC2 实例上远程执行脚本, 以将数据发送到审核系统.  
B. 使用 EC2 Auto Scaling 生命周期挂钩执行自定义脚本, 以便在启动和终止实例时将数据发送到审核系统.  
C. 使用 EC2 Auto Scaling 启动配置通过用户数据执行自定义脚本, 以便在启动和终止实例时将数据发送到审核系统.  
D. 在实例操作系统上执行自定义脚本, 以将数据发送到审核系统.  
将脚本配置为在实例启动和终止时由 EC2 Auto Scaling 组执行.

答案:B

Q231. 公司需要为其本地数据库服务器提供持久的备份存储解决方案, 同时确保本地应用程序保持对这些备份的访问以快速恢复. 该公司将使用 AWS 存储服务作为这些备份的目标. 解决方案架构师正在设计具有最小运营开销的解决方案. 解决方案架构师应实施哪种解决方案?

- A. 在本地部署 AWS Storage Gateway 文件网关并将其与 Amazon S3 存储桶关联.  
B. 将数据库备份到 AWS Storage Gateway 卷网关, 并使用 Amazon S3 API 访问它.  
C. 将数据库备份文件传输到附加到 Amazon EC2 实例的 Amazon Elastic Block Store (Amazon EBS) 卷.

D. 将数据库直接备份到 AWS Snowball 设备，并使用生命周期规则将数据移至 Amazon S3 Glacier Deep Archive.

答案:A

**Q232.** 公司的 Web 服务器在具有弹性 IP 地址的公共子网中的 Amazon EC2 实例上运行.

默认安全组已分配给 EC2 实例. 默认网络 ACL 已修改为阻止所有流量. 解决方案架构师需要使 Web 服务器可以从端口 443 上的任何位置访问. 哪种步骤组合可以完成此任务? (选择两个.)

- A. 创建一个安全组，并使用一条规则允许来自源 0.0.0.0/0 的 TCP 端口 443.
- B. 创建一个带有规则的安全组，以允许 TCP 端口 443 到达目标 0.0.0.0/0.
- C. 更新网络 ACL，以允许源 0.0.0.0/0 的 TCP 端口 443.
- D. 更新网络 ACL，以允许从源 0.0.0.0/0 到目标 0.0.0.0/0 的入站/出站 TCP 端口 443.
- E. 更新网络 ACL，以允许从源 0.0.0.0/0 入站 TCP 端口 443 和到目标 0.0.0.0/0 的出站 TCP 端口 32768-65535

答案:AE

**Q233.** 一家公司在 AWS 上托管其网站. 为了满足高度变化的需求，该公司实施了 Amazon EC2 Auto Scaling.

管理层担心该公司过度配置了基础架构，尤其是在三层应用程序的前端.

解决方案架构师需要确保在不影响性能的情况下优化成本. 解决方案架构师应该怎么做才能做到这一点?

- 淘宝: 国际认证大师 微信: ANYPASS
- A. 对保留实例使用 Auto Scaling.
  - B. 将 Auto Scaling 与计划的缩放策略一起使用.
  - C. 将 Auto Scaling 与暂停恢复功能一起使用
  - D. 将 Auto Scaling 与目标跟踪缩放策略一起使用.

答案:D

**Q234.** 公司担心，正在使用的两个 NAT 实例将不再能够支持公司应用程序所需的流量.

解决方案架构师希望实现一种高度可用的容错并自动扩展的解决方案.

解决方案架构师应该建议什么?

- A. 删除两个 NAT 实例，并用同一可用区中的两个 NAT 网关替换它们.
- B. 将 Auto Scaling 组与网络负载平衡器一起用于不同可用区域中的 NAT 实例.
- C. 删除两个 NAT 实例，并用不同可用区中的两个 NAT 网关替换它们.
- D. 用不同可用区中的竞价型实例替换这两个 NAT 实例，并部署网络负载均衡器.

答案:C

**Q235.** 解决方案架构师正在优化本地数据中心中运行在 Microsoft Windows Server 上的旧版文档管理应用程序. 该应用程序将大量文件存储在网络文件共享上. 首席信息官希望通过将本地存储移至 AWS 来减少本地数据中心的占地面积并最大程度降低存储成本.

解决方案架构师应怎么做才能满足这些要求?

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- A. 设置一个 AWS Storage Gateway 文件网关.
- B. 设置 Amazon Elastic File System (Amazon EFS)
- C. 将 AWS Storage Gateway 设置为卷网关
- D. 设置一个 Amazon Elastic Block Store (Amazon EBS) 卷.

答案:A

**Q236.** 公司每天都在处理数据.

操作结果存储在 Amazon S3 存储桶中, 每天分析一周, 然后必须立即保持访问状态以进行偶发分析, 对于当前配置, 有什么最省钱的存储解决方案?

- A. 配置生命周期策略以在 30 天后删除对象
- B. 配置生命周期策略, 以在 30 天后将对象转换到 Amazon S3 Glacier.
- C. 配置生命周期策略以在 30 天后将对象过渡到 Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
- D. 配置生命周期策略, 以在 30 天后将对象过渡到 Amazon S3 一次区域不频繁访问 (S3 One Zone-IA) .

答案:A

**Q237.** 最近对公司 IT 支出的分析表明, 需要降低备份成本. 该公司的首席信息官希望通过消除使用物理备份磁带来简化本地备份基础架构并降低成本. 公司必须保留在本地备份应用程序和工作流程中的现有投资.

解决方案架构师应该建议什么? 国际认证大师 微信: ANYPASS

- A. 设置 AWS Storage Gateway 以使用 NFS 界面与备份应用程序连接.
- B. 设置使用 NFS 接口与备份应用程序连接的 Amazon EFS 文件系统
- C. 设置一个使用 iSCSI 接口与备份应用程序连接的 Amazon EFS 文件系统
- D. 设置 AWS Storage Gateway 以使用 iSCSI 虚拟磁带库 (VTL) 接口与备份应用程序连接.

答案:D

**Q238.** 一家公司希望将其数据复制到 AWS 以便在发生灾难时进行恢复. 如今, 系统管理员拥有将数据复制到 NFS 共享的脚本, 应用程序管理员需要以低延迟访问单个备份文件, 以处理处理中的错误.

解决方案架构师应建议哪些以满足这些要求?

- A. 修改脚本以将数据复制到 Amazon S3 存储桶, 而不是本地 NFS 共享
- B. 修改脚本以将数据复制到 Amazon S3 Glacier 存档, 而不是本地 NFS 共享
- C. 修改脚本以将数据复制到 Amazon Elastic File System (Amazon EFS) 卷, 而不是本地 NFS 共享.
- D. 修改脚本以将数据复制到适用于 File Gateway 虚拟设备的 AWS Storage Gateway, 而不是本地 NFS 共享.

答案:D

**Q239.** 解决方案架构师正在设计用于新的 Web 应用程序的存储体系结构, 该应用程序用于简化和查看工程图.

所有应用程序组件都将部署在 AWS 基础架构上. 应用程序设计必须支持缓存, 以最大程度地减少用户等待工程图加载的时间.

该应用程序必须能够存储 PB 的数据. 解决方案架构师应使用哪种存储和缓存组合?

- A. 使用 Amazon CloudFront 的 Amazon S3
- B. 使用 Amazon ElastiCache 的 Amazon S3 Glacier
- C. 使用 Amazon CloudFront 的 Amazon Elastic Block Store (Amazon EBS) 卷
- D. 具有 Amazon ElastiCache 的 AWS Storage Gateway

答案:A

**Q240.** 一家开发 Web 应用程序的公司已在多个区域启动了数百个应用程序负载平衡器 (ALB). 该公司希望在其防火墙设备上创建一个允许列表 (或所有负载平衡器的 IP).

解决方案架构师正在寻找一种一次性的, 高度可用的解决方案来解决此请求, 这也将有助于减少防火墙所需的 IP 数量. 解决方案架构师应建议哪些以满足这些要求?

- A. 创建一个 AWS Lambda 函数以跟踪不同区域中所有 ALB 的 IP. 继续刷新此列表.
- B. 设置具有弹性 IP 的网络负载平衡器 (NLB).
- 注册所有 ALB 的专用 IP 作为此 NLB 的目标.
- C. 启动 **AWS Global Accelerator** 并为所有区域创建端点.
- 将不同区域中的所有 ALB 注册到相应的端点
- D. 设置一个 Amazon EC2 实例, 为该 EC2 实例分配一个弹性 IP, 然后将该实例配置为代理, 以将流量转发到所有 ALB.

答案:C

**Q241.** 一家公司最近使用 AWS Direct Connect 实现了混合云连接, 并将数据迁移到 Amazon S3. 该公司正在寻找一种完全托管的解决方案, 该解决方案将自动化并加速本地存储系统和 AWS 存储服务之间的数据复制. 解决方案架构师应建议使用哪种解决方案来保护数据私有?

- A. 将 AWS DataSync 代理部署到本地环境.  
配置同步作业以复制数据并将其与 AWS 服务终端节点连接.
- B. 为本地环境部署一个 AWS DataSync 代理.  
计划批处理作业以将时间点快照复制到 AWS.
- C. 为本地环境部署一个 AWS Storage Gateway 卷网关.  
配置它以在本地存储数据, 然后将时间点快照异步备份到 AWS.
- D. 为本地环境部署一个 AWS Storage Gateway 文件网关.  
配置它以在本地存储数据, 然后将即时点快照异步备份到 AWS.

答案:A

**Q242.** 一家公司的本地数据中心的存储容量已用完. 该公司希望将其存储基础架构迁移到 AWS, 同时将带宽成本降至最低.

该解决方案必须允许立即获取数据而无需任何额外费用.

如何满足这些要求?

A. 部署 Amazon S3 Glacier Vault 并启用快速检索.

为工作负载启用预配置的检索能力

B. 使用缓存的卷部署 AWS Storage Gateway.

使用 Storage Gateway 在 Amazon S3 中存储数据, 同时在本地保留频繁访问的数据子集的副本.

C. 使用存储的卷部署 AWS Storage Gateway 在本地存储数据.

使用 Storage Gateway 将数据的时间点快照异步备份到 Amazon S3

D. 部署 AWS Direct Connect 以与本地数据中心连接.

配置 AWS Storage Gateway 以在本地存储数据.

使用 Storage Gateway 将数据的即时时间快照异步备份到 Amazon S3.

答案:B

**Q243.** 一家公司正在审查其 AWS Cloud 部署, 以确保未经适当授权的任何人都无法访问其数据.

解决方案架构师的任务是识别所有打开的 Amazon S3 存储桶并记录所有 S3 存储桶配置更改.

解决方案架构师应该怎么做才能做到这一点?

A. 使用适当的规则启用 AWS Config 服务

B. 通过适当的检查启用 AWS Trusted Advisor.

C. 使用 AWS 开发工具包编写脚本以生成存储桶报告

D. 启用 Amazon S3 服务器访问日志记录并配置 Amazon CloudWatch Events.

答案:A

**Q244.** 一家公司构建了一个应用程序, 该应用程序使用户可以签入他们访问过的地方, 对这些地方进行排名并添加有关其体验的评论.

该应用程序成功, 每月用户数量迅速增加. 首席技术官担心, 支持当前基础架构的数据库可能无法在下个月处理新负载, 因为单个 MySQL 的 Amazon RDS 实例已因读取请求触发了与资源耗尽相关的警报. 解决方案架构师可以建议什么, 以最小的代码更改防止数据库层的服务中断?

A. 创建 RDS 只读副本, 并将只读流量重定向到只读副本端点.

启用多可用区部署.

B. 创建一个 Amazon EMR 集群, 并将数据迁移到复制因子为 3 的 Hadoop 分布式文件系统 (HDFS).

C. 创建一个 Amazon ElastiCache 集群, 并将所有只读流量重定向到该集群.

设置要在三个可用区中部署的群集.

D. 创建一个 Amazon DynamoDB 表来替换 RDS 实例, 并将所有只读流量重定向到 DynamoDB 表. 启用 DynamoDB Accelerator 以减轻主表的流量.

答案:A

**Q245.** 公司在 Amazon EC2 实例上运行应用程序. 该应用程序部署在 us-east-1 地区三个可用区中的专用子网中. 实例必须能够连接到互联网以下载文件. 该公司希望该设计在整个地区都高度可用. 应该采用哪种解决方案来确保不中断 Internet 连接?

- A. 在每个可用区的专用子网中部署 NAT 实例.
- B. 在每个可用区的公共子网中部署 NAT 网关.
- C. 在每个可用区的专用子网中部署一个传输网关.
- D. 在每个可用区的公共子网中部署 Internet 网关.

答案:B

**Q246.** 一家公司已将本地 Oracle 数据库迁移到 us-east-1 Region 中的 Amazon RDS (或 Oracle Multi-AZ 数据库实例).

解决方案架构师正在设计一种灾难恢复策略, 以在 us-west-2 区域中配置数据库, 以防在 us-east-1 区域中数据库不可用. 设计必须确保在 us-west-2 区域中最多配置 2 小时, 并且数据丢失窗口不超过 3 小时.

如何满足这些要求?

- A. 编辑数据库实例并在 us-west-2 中创建一个只读副本.  
在需要激活灾难恢复环境的情况下, 将只读副本升级为 us-west-2 中的主副本.
- B. 选择“多区域”选项以在 us-west-2 中置备一个备用实例.  
如果需要创建灾难恢复环境, 备用实例将自动升级为 us-west-2 中的 master 实例.
- C. 拍摄数据库实例的自动快照, 每 3 小时将其复制到 us-west-2.  
如果需要激活灾难恢复环境, 请还原最新快照以在 us-west-2 中置备另一个数据库实例.
- D. 在多个 AWS 区域中创建多主机读/写实例. 在 us-east-1 和 us-west-2 中选择 VPC 进行部署.  
保持 us-west-2 中的主读/写实例可用, 以避免不得不激活灾难恢复环境.

答案:A

**Q247.** 公司的应用程序带有基于 REST 的接口, 该接口允许从第三方供应商近实时地接收数据. 一旦收到, 应用程序将处理并存储数据以进行进一步分析.

该应用程序正在 Amazon EC2 实例上运行.

将数据发送到应用程序时, 第三方供应商已收到许多 503 服务不可用错误.

当数据量激增时, 计算能力达到其最大限制, 并且应用程序无法处理所有请求.

解决方案架构师应建议采用哪种设计来提供更具扩展性的解决方案?

- A. 使用 Amazon Kinesis Data Streams 摄取数据.  
使用 AWS Lambda 函数处理数据.
- B. 在现有应用程序顶部使用 Amazon API Gateway.  
为第三方供应商创建一个具有配额限制的使用计划.
- C. 使用 Amazon Simple Notification Service (Amazon SNS) 提取数据.  
将 EC2 实例放在应用程序负载均衡器后面的 Auto Scaling 组中.
- D. 将应用程序重新包装为容器.  
通过 EC2 启动类型和 Auto Scaling 组, 使用 Amazon Elastic Container Service (Amazon ECS) 部署应用程序.

答案:A

**Q248.** 公司必须在 30 天内将 20 TB 的数据从数据中心迁移到 AWS 云. 该公司的网络带宽限制为 15 Mbps, 利用率不能超过 70%. 解决方案架构师应该怎么做才能满足这些要求?

- A. 使用 AWS Snowball.
- B. 使用 AWS DataSync.
- C. 使用安全的 VPN 连接.
- D. 使用 Amazon S3 传输加速.

答案:A

**Q249.** 一家公司最近在 us-east-1 地区的两个可用区中部署了两层应用程序.

数据库部署在专用子网中, 而 Web 服务器部署在公共子网中.

Internet 网关已连接到 VPC. 该应用程序和数据库在 Amazon EC2 实例上运行.

数据库服务器无法访问 Internet 上的补丁. 解决方案架构师需要设计一种解决方案, 以最小的操作开销维护数据库安全性.

哪种解决方案满足这些要求?

- A. 在每个可用区的公共子网内部署 NAT 网关 并将其与弹性 IP 地址关联.  
更新专用子网的路由表以将其用作默认路由.
- B. 在每个可用区的专用子网内部署一个 NAT 网关, 并将其与弹性 IP 地址关联.  
更新专用子网的路由表以将其用作默认路由.
- C. 在每个可用区的公共子网内部署两个 NAT 实例, 并将它们与弹性 IP 地址关联.  
更新专用子网的路由表以将其用作默认路由.
- D. 在每个可用区的专用子网内部署两个 NAT 实例, 并将它们与弹性 IP 地址关联.  
更新专用子网的路由表以将其用作默认路由.

答案:A

**Q250.** 解决方案架构师必须为正在从本地迁移到 AWS 的持久数据库设计解决方案.

根据数据库管理员的说法, 该数据库需要 64,000 IOPS. 如果可能, 数据库管理员希望使用单个 Amazon Elastic Block Store (Amazon EBS) 卷来托管数据库实例.

哪种解决方案有效满足数据库管理员的条件?

- A. 使用 13 个 I/O 优化系列中的实例, 并利用本地临时存储来满足 IOPS 要求.
- B. 创建一个附加了 Amazon EBS 预置 IOPS SSD (io1) 卷的基于 Nitro 的 Amazon EC2 实例. 将卷配置为具有 64,000 IOPS.
- C. 创建一个 Amazon Elastic File System (Amazon EFS) 卷并将其映射到数据库实例, 并使用该卷实现数据库所需的 IOPS.
- D. 分配两卷, 并为每卷分配 32,000 IOPS. 在操作系统级别创建一个逻辑卷, 该逻辑卷将两个卷聚合在一起以达到 IOPS 要求.

答案:B

**Q251.** 一家公司最近启动了其网站，向其全球用户群提供内容。该公司希望通过利用附加了 Amazon EC2 实例的 Amazon CloudFront 来存储和加速向其用户的静态内容交付。解决方案架构师应如何优化应用程序的高可用性？

- A. 将 Lambda @ Edge 用于 CloudFront。
- B. 对 CloudFront 使用 Amazon S3 Transfer Acceleration。
- C. 在另一个可用区中配置另一个 EC2 实例作为源组的一部分。
- D. 将另一个 EC2 实例配置为同一可用区中原始服务器群集的一部分。

答案:C

**Q252.** 一家公司计划在 AWS 上构建新的 Web 应用程序。该公司预计一年中的大部分时间都是可预测的流量，偶尔还会有很高的流量。Web 应用程序必须具有高可用性，并具有最小的延迟容错能力。解决方案架构师应建议哪些以满足这些要求？

- A. 使用 Amazon Route 53 路由策略将请求分发到两个 AWS 区域，每个区域均具有一个 Amazon EC2 实例。
- B. 将 Auto Scaling 组中的 Amazon EC2 实例与跨多个可用区的 Application Load Balancer 一起使用。
- C. 将群集放置组中的 Amazon EC2 实例与跨多个可用区的 Application Load Balancer 一起使用。
- D. 在群集放置组中使用 Amazon EC2 实例，并将群集放置组包括在新的 Auto Scaling 组中。

答案:B

**Q253.** 公司希望将工作负载迁移到 AWS。

首席信息官认为将存储在云中的所有数据静态加密。

该公司希望对加密密钥生命周期管理进行完全控制。公司必须能够独立于 AWS CloudTrail 立即删除密钥材料并审核密钥使用情况。

所选服务应与将在 AWS 上使用的其他存储服务集成。哪些服务满足这些安全要求？

- A. AWS CloudHSM 与 CloudHSM 客户端
- B. 带有 AWS CloudHSM 的 AWS Key Management Service (AWS KMS)
- C. 具有外部密钥材料来源的 AWS 密钥管理服务 (AWS KMS)
- D. 具有 AWS 管理的客户主密钥 (CMK) 的 AWS Key Management Service (AWS KMS)

答案:B

**Q254.** 一家公司正在寻找一种可以将旧新闻素材中的视频档案存储在 AWS 中的解决方案。该公司需要将成本降到最低，并且很少需要还原这些文件。当需要这些文件时，它们必须在最多五分钟内可用。

什么是最具成本效益的解决方案？

- A. 将视频档案存储在 Amazon S3 Glacier 中，并使用快速检索。
- B. 将视频档案存储在 Amazon S3 Glacier 中并使用标准检索。
- C. 将视频档案存储在 Amazon S3 Standard-Infrequent Access (S3 Standard-IA) 中。
- D. 将视频档案存储在 Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) 中。

答案:A

Q255. 一家公司希望将 Amazon S3 用作其本地数据集的二级副本.  
该公司很少需要访问此副本.  
存储解决方案的成本应最小.  
哪种存储解决方案满足这些要求?

- A. S3 标准
- B. S3 智能分层
- C. S3 标准-不频繁访问 (S3 Standard-IA)
- D. S3 一区不频繁访问 (S3 一区-IA)

答案:D

Q256. 一家公司已启用 AWS CloudTrail 日志, 以为其每个开发人员账户将日志文件传送到 Amazon S3 存储桶.  
该公司已经创建了一个中央 AWS 账户来简化管理和审核审查.  
内部审核员需要访问 CloudTrail 日志, 但是需要限制所有开发人员账户用户的访问.  
解决方案必须是安全且经过优化的. 解决方案架构师应如何满足这些要求?

- A. 在每个开发人员账户中配置一个 AWS Lambda 函数, 以将日志文件复制到中央帐户.  
在中央帐户中为审计员创建一个 IAM 角色.  
将提供只读权限的 IAM 策略附加到存储桶.
- B. 从每个开发人员账户配置 CloudTrail, 以将日志文件传递到中央帐户中的 S3 存储桶.  
在中央帐户中为审核员创建一个 IAM 用户.  
附加一个 IAM 策略, 为存储桶提供完全权限.
- C. 从每个开发人员账户配置 CloudTrail, 以将日志文件传递到中央帐户中的 S3 存储桶.  
在中央帐户中为审计员创建一个 IAM 角色.  
将提供只读权限的 IAM 策略附加到存储桶.
- D. 在中央帐户中配置一个 AWS Lambda 函数, 以从每个开发人员账户中的 S3 存储桶中复制日志文件.  
在中央帐户中为审核员创建一个 IAM 用户.  
附加一个 IAM 策略, 为存储桶提供完全权限.

答案:C

原始答案为 A , 现更正为 C ,

Q257. 一家公司拥有一个将消息发布到 Amazon SQS 的应用程序. 另一个应用程序轮询队列并以 I/O 密集型操作处理消息. 该公司具有服务级别协议 (SLA), 该协议指定了在接收消息和响应用户之间可以经过的最长时间. 由于消息数量的增加, 公司难以始终如一地满足其 SLA.  
解决方案架构师应采取什么措施来帮助改善应用程序的处理时间并确保其可以处理任何级别的负载?

- A. 从用于处理的实例创建 Amazon Machine Image (AMI) .  
终止实例并将其替换为更大的尺寸.

- B. 从用于处理的实例创建 Amazon Machine Image (AMI).  
终止实例并将其替换为 Amazon EC2 专用实例
- C. 从用于处理的实例创建 Amazon Machine image (AMI).  
在启动配置中使用该映像创建一个 Auto Scaling 组.  
使用目标跟踪策略配置该组, 以使我们的总 CPU 利用率保持在 70% 以下.
- D. 从用于处理的实例创建 Amazon Machine Image (AMI).  
在启动配置中使用该映像创建一个 Auto Scaling 组.  
根据 SQS 队列中最旧邮件的年龄, 使用目标跟踪策略配置组.

答案:D

**Q258.** 一家公司计划部署运行 Amazon Aurora 的 Amazon RDS 数据库实例. 该公司的备份保留政策要求为 90 天. 解决方案架构师应建议哪种解决方案?

- A. 在创建 RDS 数据库实例时, 将备份保留期设置为 90 天
- B. 配置 RDS 以将自动快照复制到用户管理的 Amazon S3 存储桶, 并将生命周期策略设置为 90 天后删除.
- C. 创建一个 AWS Backup 计划以执行 RDS 数据库的每日快照, 并将保留时间设置为 90 天.  
创建一个 AWS Backup 作业以安排每天执行备份计划
- D. 将每日计划的事件与 Amazon CloudWatch Events 一起使用以执行自定义 AWS Lambda 函数, 该函数可复制 RDS 自动快照的副本清除 90 天以上的快照

答案:C

**Q259.** 一家公司正在使用磁带备份解决方案将其关键应用程序数据存储在异地.  
每日数据量约为 50 TB.

该公司需要将备份保留 7 年, 以用于监管目的. 很少访问备份, 如果需要恢复备份, 通常会给出一周的通知.  
该公司现在正在考虑基于云的选项, 以降低存储成本和管理磁带的运营负担.  
该公司还希望确保过渡(将磁带备份到云端)将中断降到最低.  
哪种存储解决方案最符合成本效益?

- A. 使用 Amazon Storage Gateway 备份到 Amazon Glacier Deep Archive
- B. 使用 AWS Snowball Edge 直接将备份与 Amazon S3 Glacier 集成.
- C. 将备份数据复制到 Amazon S3 并创建生命周期策略以将数据移动到 Amazon S3 Glacier
- D. 使用 Amazon Storage Gateway 备份到 Amazon S3 并创建生命周期策略以将备份移至 Amazon S3 Glacier

答案:D

**Q260.** 一家公司所依赖的应用程序在正常流量期间至少需要 4 个 Amazon EC2 实例, 并且在高峰负载期间必须扩展到 12 个 EC2 实例. 该应用程序对企业至关重要, 并且必须高度可用哪个解决方案可以满足这些要求?

- A. 将 EC2 实例部署在 Auto Scaling 组中.  
将最小值设置为 4, 将最大值设置为 M, 在可用区 A 中设置 2, 在可用区 B 中设置 2

B.将 EC2 实例部署在 Auto Scaling 组中.

将最小值设置为 4, 将最大值设置为 12, 所有 4 个设置在可用区 A 中

C.在 Auto Scaling 组中部署 EC2 实例.

将最小值设置为 8, 将最大值设置为 12, 在可用区 A 中设置 4, 在可用区 B 中设置 4

D.在 Auto Scaling 组中部署 EC2 实例.

在可用区 A 中将最小值设置为 8, 将最大值设置为 12

答案:A

**Q261.** 一家公司计划将其基于虚拟服务器的工作负载迁移到 AWS 上. 该公司拥有由应用程序服务器支持的面向 Internet 的负载均衡器. 应用程序服务器依赖于 Internet 托管的存储库中的补丁程序, 解决方案架构师建议将哪些服务托管在公共子网中? (选择两个.)

A.NAT 网关

B.Amazon RDS 数据库实例

C.应用程序负载平衡器

D.Amazon EC2 应用程序服务器

E.Amazon 弹性文件系统 (Amazon EFS) 卷

答案:AC

**Q262.** 应用程序在 Amazon EC2 实例上运行. 该应用程序所需的敏感信息存储在 Amazon S3 存储桶中.

需要保护存储桶免受 Internet 访问, 同时仅允许 VPC 内的服务访问存储桶.

存档的解决方案应采取哪种动作组合来完成此任务" (选择两个).

A.为 Amazon S3 创建 VPC 终端节点.

B.在存储桶上启用服务器访问日志记录

C.应用存储桶策略以限制对 S3 端点的访问.

D.向具有敏感信息的存储桶中添加一个 S3 ACL

E.限制使用 IAM 策略的用户使用特定存储桶

答案:AC

**Q263.** 解决方案架构师正在为将提供公共 API 访问的应用程序设计多区域灾难恢复解决方案.

该应用程序将结合使用带有用户数据脚本的 Amazon EC2 实例来加载应用程序代码和一个用于 MySQL 数据库的 Amazon RDS.

恢复时间目标 (RTO) 为 3 小时, 恢复点目标 (RPO) 为 24 小时.

哪种架构能够以最低的成本满足这些要求?

A.使用应用程序负载平衡器进行区域故障转移.

使用 userdata 脚本部署新的 EC2 实例.

在每个区域中部署单独的 RDS 实例

B.使用 Amazon Route 53 进行区域故障转移.

使用 userdata 脚本部署新的 EC2 实例.

在备份区域中创建 RDS 实例的只读副本

- C. 使用 Amazon API Gateway 进行公共 API 和区域故障转移.  
使用 **userdata** 脚本部署新的 EC2 实例.  
在备份区域中创建 RDS 实例的 MySQL 只读副本
- D. 使用 Amazon Route 53 进行区域故障转移.  
使用用于 API 的 **userdata** script 部署新的 EC2 实例，并每天创建 RDS 实例的快照以进行备份.  
将快照复制到备份区域

答案:D

Q264. 解决方案架构师正在使用 Amazon API Gateway 设计一个新 API，它将接收来自用户的需求.

请求的数量变化很大，可能要经过几个小时才能收到一个单独的请求.

数据处理将异步进行，但应在发出请求后的几秒钟内完成

解决方案架构师应使用哪种 API 调用 API 以最低的成本交付需求？

- A.AWS Glue 作业
- B.AWS Lambda 函数
- C.托管在 Amazon Elastic Kubernetes 服务（Amazon EKS）中的容器化服务
- D.使用 Amazon EC2 托管在 Amazon ECS 中的容器化服务

答案:B

Q265. 开发团队需要托管一个网站，其他团队可以访问该网站. 网站内容由 HTML 组成. CSS，客户端 JavaScript 和图像. 托管网站最经济有效的方法是哪种？

- 淘宝：国际认证大师 微信：ANYPASS
- A. 容器化网站并将其托管在 AWS Fargate 中
  - B. 创建一个 Amazon S3 存储桶并在那里托管网站.
  - C. 在 Amazon EC2 实例上部署 Web 服务器以托管网站.
  - D. 使用使用 Express.js 框架的 AWS Lambda 目标配置应用程序负载均衡器

答案:B

Q266. 公司的媒体和应用程序文件需要在内部共享. 当前使用 Active Directory 对用户进行身份验证，并可以从 Microsoft Windows 平台访问文件.

首席执行官希望保持相同的用户权限，但希望公司在达到存储容量限制时改进流程.

解决方案架构师应该建议什么？

- A. 设置公司的 Amazon S3 存储桶，并移动媒体和应用程序文件.
- B. 为 Windows 文件服务器配置 Amazon FSx，并移动所有媒体和应用程序文件.
- C. 配置 Amazon Elastic File System（Amazon EFS）并移动所有媒体和应用程序文件.
- D. 在 Windows 上设置 Amazon EC2，附加多个 Amazon Elastic Block Store（Amazon EBS）卷，然后移动所有媒体和应用程序文件.

答案:B

**Q267.** 一家公司正在将其遗留工作负载转移到 AWS 云. 首次创建工作负载文件时, 它们将通过 Amazon EC2 实例共享, 附加和频繁访问.

随着时间的流逝, 文件会偶尔被访问

解决方案架构师应该建议什么?

- A. 使用带有附加的 Amazon Elastic Block Store (Amazon EBS) 数据卷的 Amazon EC2 实例存储数据
- B. 使用 AWS Storage Gateway 卷网关存储数据并将很少访问的数据导出到 Amazon S3 存储
- C. 使用 Amazon Elastic File System (Amazon EFS) 存储数据, 并为很少访问的数据启用生命周期管理
- D. 使用启用了 S3 生命周期策略的 Amazon S3 存储数据, 以将数据移至 S3 Standard-Infrequent Access (S3 Standard-IA)

答案:C

**Q268.** 一家公司正在 AWS 内部署一个多实例应用程序, 该实例需要最小的实例之间的延迟.

解决方案架构师应该建议什么?

- A. 将 Auto Scaling 组与群集放置组一起使用.
- B. 在同一 AWS 区域中的单个可用区中使用 Auto Scaling 组.
- C. 将 Auto Scaling 组与同一 AWS 区域中的多个可用区配合使用.
- D. 使用具有多个 Amazon EC2 专用主机的网络负载均衡器作为目标

答案:A

淘宝: 国际认证大师 微信: ANYPASS

**Q269.** 公司每天从各种来源接收结构化和半结构化数据. 解决方案架构师需要设计一种利用大数据处理框架的解决方案. 可以使用 SQL 查询和商业智能工具访问数据. 解决方案架构师应建议什么来构建 MOST 高性能解决方案?

- A. 使用 AWS Glue 处理数据并使用 Amazon S3 存储数据
- B. 使用 Amazon EMR 处理数据并使用 Amazon Redshift 存储数据
- C. 使用 Amazon EC2 处理数据并使用 Amazon Elastic Block Store (Amazon EBS) 存储数据
- D. 使用 Amazon Kinesis Data Analytics 处理数据并使用 Amazon Elastic File System (Amazon EFS) 存储数据

答案:A

**Q270.** 公司正在设计一个使用 Amazon S3 存储桶存储静态图像的网站. 该公司希望所有未来的请求都具有品尝者的响应时间, 同时减少延迟和成本.

解决方案架构师应建议哪种服务配置?

- A. 在 Amazon S3 前面部署 NAT 服务器.
- B. 在 Amazon S3 之前部署 Amazon CloudFront.
- C. 在 Amazon S3 前面部署网络负载平衡器.
- D. 配置自动缩放以自动调整网站的容量.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

答案:B

**Q271.** 解决方案架构师应该怎么做才能确保上传到 Amazon S3 存储桶的所有对象都经过加密?

- A.更新存储桶策略以拒绝 PutObject 没有设置 s3 x-amz-acl 标头的情况
- B.将存储桶策略更新为拒绝, 如果 PutObject 没有将 s3 x-amz-acl 标头设置为 private
- C.将存储桶策略更新为拒绝, 如果 PutObject 没有将 aws SecureTransport 标头设置为 true
- D.更新存储桶策略以拒绝 PutObject 没有设置 x-amz-server-side-encryption 标头的情况

答案:D

**Q272.** 一家公司在 AWS 上运行高性能计算 (HPC) 工作负载. 工作负载要求低延迟网络性能和高网络吞吐量以及紧密耦合的节点到节点通信.

Amazon EC2 实例的大小适合计算和存储容量, 并使用默认选项启动.

解决方案架构师应提出什么建议来改善工作负载的性能?

- A.启动 Amazon EC2 实例时选择一个集群放置组
- B.启动 Amazon EC2 实例时选择专用实例租赁
- C.启动 Amazon EC2 实例时选择 Elastic Inference 加速器
- D.在启动 Amazon EC2 实例时选择所需的容量预留.

答案:A

**Q273.** 公司的动态网站使用美国的本地服务器托管. 该公司正在欧洲推出其产品, 并希望为新的欧洲用户优化站点加载时间.

该网站的后端必须保留在美国. 该产品将在几天内发布, 需要立即解决方案

解决方案架构师应该建议什么?

- A.在 us-east-1 中启动 Amazon EC2 实例并将网站迁移到该实例
- B.将网站移至 Amazon S3. 在区域之间使用跨区域复制.
- C.将 Amazon CloudFront 与指向本地服务器的自定义来源一起使用
- D.使用指向本地服务器的 Amazon Route 53 地理邻近路由策略

答案:C

**Q274.** 一家公司正在构建媒体共享应用程序, 并决定使用 Amazon S3 进行存储. 上载媒体文件后, 公司将开始一个多步骤过程, 以创建缩略图, 识别图像中的对象, 将视频转码为标准格式和分辨率, 以及提取元数据并将其存储到 Amazon DynamoDB 表中.

元数据用于搜索和导航. 通信量是可变的解决方案必须能够扩展以应对负载高峰, 而没有不必要的支出. 解决方案架构师应建议什么来支持此工作负载?

- A.将处理内置到用于将内容上传到 Amazon S3 的网站或移动应用程序中.  
上载对象后, 将所需数据保存到 DynamoDB 表中
- B.当对象存储在 S3 存储桶中时, 触发 AWS Step Functions.  
让“步骤功能”执行处理对象所需的步骤, 然后将元数据写入 DynamoDB 表
- C.当对象存储在 S3 存储桶中时, 触发 AWS Lambda 函数.

让 Lambda 函数启动 AWS Batch 以执行处理对象的步骤.

完成后将对象数据放置在 DynamoDB 表中

D.当对象上载到 Amazon S3 时, 触发 AWS Lambda 函数以将初始条目存储在 DynamoDB 表中. 使用在 Auto Scaling 组中的 Amazon EC2 实例上运行的程序来轮询索引以进行未处理, 使用该程序执行处理

答案:B

Q275. 一家公司最近更新了其内部安全标准. 公司现在必须确保使用内部安全专家创建并定期轮换的密钥对所有 Amazon S3 存储桶和 Amazon Elastic Block Store (Amazon EBS) 卷进行加密. 该公司正在寻找一种基于软件的本地 AWS 服务来实现此目标. 解决方案架构师应建议什么作为解决方案?

- A. 使用带有客户主密钥 (CMK) 的 AWS Secrets Manager 来存储主密钥材料, 并应用例程来定期创建新的 CMK, 并在 AWS Secrets Manager 中将其替换.
- B. 将 AWS Key Management Service (AWS KMS) 与客户主密钥 (CMK) 一起使用以存储主密钥材料, 并应用路由以定期重新创建新密钥并将其替换在 AWS KMS 中.
- C. 使用带有客户主密钥 (CMK) 的 AWS CloudHSM 集群来存储主密钥材料, 并应用例程并定期重新创建新密钥, 并将其替换到 CloudHSM 集群节点中.
- D. 将 AWS Systems Manager 参数存储与客户主密钥 (CMK) 密钥一起使用来存储主密钥材料, 并应用例程以定期重新创建新的并将其替换在参数存储中.

答案:B

Q276. ~~解决方案架构师必须设计一个使用 Amazon CloudFront 和 Amazon S3 来存储静态网站的解决方案.~~

公司安全政策要求 AWS WAF 检查所有网站流量. 解决方案架构师应如何满足这些要求?

- A. 配置 S3 存储桶策略以仅接受来自 AWS WAF Amazon Resource Name (ARN) 的请求
- B. 将 Amazon CloudFront 配置为将所有传入请求转发到 AWS WAF, 然后再从 S3 来源请求内容,
- C. 配置一个安全组, 该安全组允许 Amazon CloudFront IP 地址仅访问 Amazon S3 将 AWS WAF 与 CloudFront 相关联.
- D. 将 Amazon CloudFront 和 Amazon S3 配置为使用源访问身份 (OAI) 来限制对 S3 存储桶的访问. 在分发上启用 AWS WAF.

答案:D

Q277. 一家公司已使用 AWS Direct Connect 链接将 1 PB 的数据从主机托管设施复制到 us-1 区域中的 Amazon S3 存储桶.

该公司现在希望将数据复制到 us-west-2 Region 中的另一个 S3 存储桶. 托管设施不允许使用 AWS Snowball. 解决方案架构师应该推荐什么来实现这一目标?

- A. 订购 Snowball Edge 设备将数据从一个地区复制到另一地区.
- B. 使用 S3 控制台将内容从源 S3 存储桶传输到目标 S3 存储桶.
- C. 使用 aws s3 sync 命令将数据从源存储桶复制到目标存储桶.
- D. 添加跨区域复制配置, 以跨不同 Region 中的 S3 存储桶复制对象.

答案:A

Q278. 一家公司聘请了一位新的云工程师，该工程师不应该访问名为 Company Confidential 的 Amazon S3 存储桶。

云工程师必须能够读取和写入名为 AdminTools 的 S3 存储桶。

哪个 IAM 策略将满足这些要求？

A.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListBucket",
            "Resource": "arn:aws:s3:::AdminTools"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

淘宝：国际认证大师 微信：ANYPASS

B.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListBucket",  
            "Resource": [  
                "arn:aws:s3:::AdminTools",  
                "arn:aws:s3:::CompanyConfidential/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": "arn:aws:s3:::CompanyConfidential"  
        }  
    ]  
}
```

淘宝：国际认证大师 微信：ANYPASS

C.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::CompanyConfidential/*",  
                "arn:aws:s3:::CompanyConfidential"  
            ]  
        }  
    ]  
}
```

淘宝：国际认证大师 微信：ANYPASS

D.

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "s3>ListBucket",
        "Resource": "arn:aws:s3:::AdminTools/*"
    },
    {
        "Effect": "Allow",
        "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],
        "Resource": "arn:aws:s3:::AdminTools/"
    },
    {
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::CompanyConfidential",
            "arn:aws:s3:::CompanyConfidential/*",
            "arn:aws:s3:::AdminTools",
            "arn:aws:s3:::AdminTools/*"
        ]
    }
]
```

淘宝：国际认证大师 微信：ANYPASS

答案:A

**Q279.** 一个工程团队正在开发和部署 AWS Lambda 功能。团队需要在 AWS IAM 中创建角色并管理策略，以配置 Lambda 函数的权限。  
应该如何配置团队的权限，以便他们也遵循最小特权的概念？

- A. 创建一个 IAM 角色，并附加一个托管策略。  
允许工程团队和 Lambda 函数担当此角色
- B. 为工程团队创建一个 IAM 组，并附加一个 IAMFullAccess 策略。  
将团队中的所有用户添加到该 IAM 组
- C. 为 Lambda 函数创建执行角色。  
附加具有特定于这些 Lambda 函数的权限边界的托管策略
- D. 创建一个 IAM 角色，并附加一个托管策略，该策略具有特定于 Lambda 函数的权限边界。  
让工程团队承担这个角色。

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

答案:D

Q280. 公司需要在其本地环境和 AWS 之间建立安全连接. 此连接不需要高带宽, 将处理少量流量. 连接应快速建立.

建立这种连接的最经济有效的方法是什么?

- A. 实施客户端 VPN
- B. 实施 AWS Direct Connect
- C. 在 Amazon EC2 53D 上实施堡垒主机.
- D. 实施一个 AWS Site-to-Site VPN 连接.

答案:D

Q281. 公司正在构建付款应用程序, 即使在区域服务中断期间, 该应用程序也必须高度可用.

解决方案架构师必须设计一个易于在其他 AWS 区域中复制和使用的数据存储解决方案.

该应用程序还需要低延迟的原子性, 一致性, 隔离性和持久性 (ACID) 事务, 这些事务必须立即可用以生成报告.

开发团队还需要使用 SQL.

哪种数据存储解决方案满足这些要求?

- A. Amazon Aurora 全球数据库
- B. Amazon DynamoDB 全局表
- C. 具有跨区域复制和 Amazon Athena 的 Amazon S3
- D. 具有 Amazon Elastic Block Store (Amazon EBS) 快照复制的 Amazon EC2 实例上的 MySQL

答案:C

Q282. 解决方案架构师正在使用 Amazon S3 来设计新的数字媒体应用程序的存储架构.

媒体文件必须能够抵抗可用区的丢失, 某些文件经常访问, 而其他文件很少以不可预测的方式访问. 解决方案架构师必须将存储和检索媒体文件的成本降至最低.

哪个存储选项符合这些要求?

- A. S3 标准
- B. S3 智能分层
- C. S3 标准-不频繁访问 (S3 Standard-IA)
- D. S3 一区不频繁访问 (S3 一区-IA)

答案:B

Q283. 公司使用旧式本地分析应用程序, 该应用程序以千兆字节的 csv 文件运行, 代表数月的数据.

旧版应用程序无法处理不断增长的 csv 文件大小, 每天都会从各种数据源向中央本地存储位置添加新的 csv 文件. 该公司希望在用户学习 AWS 分析服务的同时继续支持旧版应用程序.

为了实现这一目标, 解决方案架构师希望在本地和 Amazon S3 中维护所有 csv 文件的两个同步副本.

解决方案架构师应建议哪种解决方案?

A. 在本地部署 AWS DataSync.

配置 DataSync 以在公司的本地存储和公司的 S3 存储桶之间连续复制 csv 文件

B. 部署本地文件网关.

配置数据源以将 csv 文件写入文件网关.

将旧版分析应用程序指向文件网关.

文件网关应将 csv 文件复制到 Amazon S3

C. 部署本地卷网关.

配置数据源以将 csv 文件写入卷网关.

将旧版分析应用程序指向卷网关.

卷网关应将数据复制到 Amazon S3.

D. 在本地部署 AWS DataSync.

配置 DataSync 以在本地和 Amazon Elastic File System (Amazon EFS) 之间连续复制 csv 文件.

启用从 Amazon EFS 到公司 S3 存储桶的复制.

答案:A

**Q284.** 一个应用程序允许公司总部的用户访问产品数据. 产品数据存储在 Amazon RDS MySQL 数据库实例中. 运营团队已隔离了应用程序性能下降的问题，并希望将读取流量与写入流量分开. 解决方案架构师需要快速优化应用程序的性能.

解决方案架构师应该建议什么？

A. 将现有数据库更改为多可用区部署.

服务来自主要可用区的读取请求.

B. 将现有数据库更改为多可用区部署.

服务来自辅助可用区的读取请求.

C. 为数据库创建只读副本.

使用一半的计算和存储资源作为源数据库配置只读副本.

D. 为数据库创建只读副本.

使用与源数据库相同的计算和存储资源配置只读副本.

答案:D

**Q285.** 一家公司希望针对季度访问的数据优化其数据存储的成本. 该公司需要在需要时具有高吞吐量，低延迟和快速访问. 解决方案架构师应推荐哪种 Amazon S3 存储类？

A. 亚马逊 S3 冰川 (S3 冰川)

B. Amazon S3 标准 (S3 标准)

C. Amazon S3 智能分层 (S3 智能分层)

D. Amazon S3 标准不频繁访问 (S3 Standard-IA)

答案:D

**Q286.** 公司要求保留其 Amazon S3 存储桶中所有版本的对象. 当前对象版本将在前 30 天内频繁访问，此后将很少访问它们，并且必须在 5 分钟内对其进行检索. 以前的对象版本需要永久保存，

很少被访问，并且可以在 1 周之内检索到。所有存储解决方案都必须具有高可用性和高度耐用性。  
解决方案架构师应建议什么，以**最具成本效益的方式**满足这些要求？

- A. 为存储桶创建一个 S3 生命周期策略，该策略将 30 天后将当前对象版本从 S3 Standard 存储移动到 S3 Glacier，并在 1 天后将先前的对象版本移动到 S3 Glacier。
- B. 为存储桶创建一个 S3 生命周期策略，该策略将 30 天后将当前对象版本从 S3 Standard 存储移动到 S3 Glacier，并在 1 天后将先前的对象版本移动到 S3 Glacier Deep Archive
- C. 为存储桶创建一个 S3 生命周期策略，该策略将 30 天后将当前对象版本从 S3 Standard 存储移动到 S3 Standard-infrequent Access (S3 Standard-IA)，并在 1 天后将先前的对象版本移动到 S3 Glacier Deep Archive
- D. 为存储桶创建 S3 生命周期策略，该策略将 30 天后将当前对象版本从 S3 标准存储移动到 S3 一个区域不频繁访问 (S3 One Zone-IA)，并在 1 天后将先前的对象版本移动到 S3 Glacier Deep Archive

答案:B

**Q287.** 公司托管其核心网络服务，包括目录服务和 DNS。在其内部数据中心。

数据中心使用 AWS Direct Connect (DX) 连接到 AWS 云，计划中的其他 AWS 账户将需要快速、经济高效且一致地访问这些网络服务

解决方案架构师应以最低的运营开销实施哪些措施来满足这些要求？

- A. 在每个新帐户中创建一个 DX 连接。  
将网络流量路由到本地服务器
- B. 在 DX VPC 中为所有必需的服务配置 VPC 端点。  
将网络流量路由到本地服务器
- C. 在每个新帐户和 DX VPC 之间创建 VPN 连接将网络流量路由到本地服务器
- D. 在账户之间配置 AWS Transit Gateway。  
将 DX 分配给传输网关，并将网络流量路由到本地服务器

答案:D

**Q288.** 一家在 AWS 上托管其 Web 应用程序的公司希望确保所有 Amazon EC2 实例、Amazon RDS 数据库实例和 Amazon Redshift 集群配置有标签。该公司希望最大程度地减少配置和操作此检查的工作量。解决方案架构师应该怎么做才能做到这一点？

- A. 使用 AWS Config 规则定义和检测未标记属性的资源
- B. 使用 Cost Explorer 来显示没有正确标记的资源手动标记这些资源。
- C. 编写 API 调用以检查所有资源是否正确分配了标签。  
定期在 EC2 实例上运行代码。
- D. 编写 API 调用以检查所有资源是否正确分配了标签。  
通过 Amazon CloudWatch 安排 AWS Lambda 函数以定期运行代码

答案:A

**Q289.** 在 Amazon EC2 实例上运行的应用程序需要访问 Amazon DynamoDB 表。

EC2 实例和 DynamoDB 表都在同一个 AWS 账户中。解决方案架构师必须配置必要的权限。哪种解决方案将允许从 EC2 实例对 DynamoDB 表的最小特权访问？

- A. 使用适当的策略创建一个 IAM 角色，以允许访问 DynamoDB 表。

**创建实例配置文件以将此 IAM 角色分配给 EC2 实例**

- B. 使用适当的策略创建一个 IAM 角色，以允许访问 DynamoDB 表。

将 EC2 实例添加到信任关系策略文档中，以使其能够担任该角色

- C. 使用适当的策略创建一个 IAM 用户，以允许访问 DynamoDB 表。

将凭证存储在 Amazon S3 存储桶中，并直接从应用程序代码中读取它们。

- D. 使用适当的策略创建一个 IAM 用户，以允许访问 DynamoDB 表。

确保应用程序将 IAM 凭据安全地存储在本地存储上，并使用它们进行 DynamoDB 调用

答案:A

**Q290.** 应用程序使用 Amazon RDS MySQL 数据库实例。

RDS 数据库的磁盘空间不足。

解决方案架构师希望在不停机的情况下增加磁盘空间。哪项解决方案能最轻松地满足这些要求？

- A. 在 RDS 中启用存储自动缩放。

- B. 增加 RDS 数据库实例大小

- C. 将 RDS 数据库实例存储类型更改为 Provisioned IOPS。

- D. 备份 RDS 数据库，增加存储容量，还原数据库并停止前一个实例

答案:A

淘宝：国际认证大师 微信：ANYPASS

**Q291.** 运营团队的标准规定，IAM 策略不应直接应用于用户。

一些新的团队成员没有遵循此标准。运营经理需要一种可以轻松识别带有附加策略的用户的方法。

解决方案架构师应该怎么做才能做到这一点？

- A. 使用 AWS CloudTrail 进行监控

- B. 创建一个每天运行的 AWS Config 规则。

- C. 将 IAM 用户更改发布到 Amazon SNS

- D. 修改用户后运行 AWS Lambda

答案:B

读 215

**Q292.** 公司拥有一个在 VPC 的专用子网内的 Amazon EC2 实例上运行的应用程序。

实例访问同一 AWS 区域中 Amazon S3 存储桶中的数据。VPC 在公共子网中包含一个 NAT 网关，

以访问 S3 存储桶。该公司希望通过替换 NAT 网关来降低成本，同时又不影响安全性或冗余性。

哪种解决方案满足这些要求？

- A. 用 NAT 实例替换 NAT 网关

- B. 用 Internet 网关替换 NAT 网关。

- C. 用网关 VPC 端点替换 NAT 网关

- D. 将 NAT 网关替换为 AWS Direct Connect 连接

答案:C

**Q293.** 一家公司正在 AWS 上设计消息驱动的订单处理应用程序. 该应用程序包含许多服务, 需要将其处理结果传达给多个使用服务.  
每个使用服务可能最多需要 5 天才能收到邮件.  
哪个过程可以满足这些要求?

- A. 应用程序将其处理结果发送到 Amazon Simple Notification Service (Amazon SNS) 主题.  
每个使用服务都订阅此 SNS 主题并使用结果
- B. 应用程序将其处理结果发送到 Amazon Simple Notification Service (Amazon SNS) 主题.  
每个使用服务都直接从其相应的 SNS 主题使用消息.
- C. 应用程序将其处理结果发送到 Amazon Simple Queue Service (Amazon SQS) 队列.  
每个使用服务均作为使用该单个 SQS 队列的 AWS Lambda 函数运行.
- D. 应用程序将其处理结果发送到 Amazon Simple Notification Service (Amazon SNS) 主题.  
为每个服务创建一个 Amazon Simple Queue Service (Amazon SQS) 队列, 并将每个队列配置为 SNS 主题的订阅者.

答案:D

**Q294.** 一家公司每月存储一次通话记录在统计上, 可以在一年内随机引用记录的数据, 但在 1 年后很少访问. 必须查询并检索早于 1 年的文件. 检索较旧文件的延迟是可以接受的. 解决方案架构师需要以最小的成本存储记录的数据.  
哪种解决方案最划算?

- A. 将单个文件存储在 Amazon S3 Glacier 中, 并将搜索元数据存储在 S3 Glacier 中创建的对象标签中.  
查询 S3 Glacier 标签并从 S3 Glacier 检索文件
- B. 在 Amazon S3 中存储单个文件 1 年后, 使用生命周期策略将文件移至 Amazon S3 Glacier.  
从 Amazon S3 或 S3 Glacier 查询和检索文件.
- C. 存档单个文件, 并将每个存档的搜索元数据存储在 Amazon S3 中.  
一年后, 使用生命周期策略将文件移至 Amazon S3 Glacier.  
通过搜索 Amazon S3 中的元数据来查询和检索文件
- D. 在 Amazon S3 中归档单个文件.  
一年后, 使用生命周期策略将文件移至 Amazon S3 Glacier.  
将搜索元数据存储在 Amazon DynamoDB 中从 DynamoDB 查询文件并从 Amazon S3 或 S3 Glacier 检索它们

答案:B

**Q295.** 一家公司拥有高度动态的批处理作业, 该作业使用许多 Amazon EC2 实例来完成它.  
该工作本质上是无状态的, 可以在任何给定时间启动和停止而不会产生负面影响, 并且通常最多需要 60 分钟才能完成. 该公司已要求解决方案架构师设计出可满足工作要求的可扩展且经济高效的解决方案.  
解决方案架构师应该建议什么?

- A. 实施 EC2 竞价型实例

- B. 购买 EC2 预留实例
- C. 实施 EC2 按需实例
- D. 在 AWS Lambda 上实施处理

答案:A

**Q296.** 在线照片应用程序使用户可以上传照片并执行图像编辑操作。该应用程序提供两类服务：免费和付费服务。付费用户提交的照片要先处理，然后再由免费用户提交。  
将照片上传到 Amazon S3，并将职位信息发送到 Amazon SQS。解决方案架构师应建议哪种配置？

- A. 使用一个 SQS FIFO 队列。  
为付费照片分配更高的优先级，以便首先处理它们
- B. 使用两个 SQS FIFO 队列：一个用于付费队列，一个用于免费队列。  
将空闲队列设置为使用短轮询，将付费队列设置为使用长轮询
- C. 使用两个 SQS 标准队列，一个为付费队列，另一个为免费队列。  
配置 Amazon EC2 实例，以优先于付费队列优先于付费队列轮询。
- D. 使用一个 SQS 标准队列。将付费照片的**可见性超时设置为零**  
配置 Amazon EC2 实例以区分可见性设置的优先级，以便首先处理付费照片

答案:C

**Q297.** 一家公司在跨不同 AWS 区域的两个 VPC 中的 Amazon EC2 实例上托管了一个应用程序。为了彼此通信，实例使用互联网进行连接。安全团队希望确保实例之间的通信不会通过 Internet 发生。  
解决方案架构师应该怎么做才能做到这一点？

- A. 创建一个 NAT 网关并更新 EC2 实例的子网的路由表
- B. 创建一个 VPC 端点并更新 EC2 实例的子网的路由表
- C. 创建一个 VPN 连接并更新 EC2 实例的子网的路由表
- D. 创建一个 VPC 对等连接并更新 EC2 实例的子网的路由表

答案:D

**Q298.** 一家公司运行生产应用程序。该应用程序从 Amazon SQS 队列读取数据并并行处理消息。  
消息量是不可预测的，并且经常具有间歇性流量。该应用程序应不间断地连续处理消息。哪种解决方案可以**最经济地**满足这些要求？

- A. 仅使用竞价型实例来处理所需的最大容量
- B. 仅使用预留实例来处理所需的最大容量
- C. 将预留实例用于基准容量，并使用竞价 Instances 处理其他容量
- D. 使用预留实例作为基准容量，并使用按需实例处理其他容量

答案:C

**Q299.** 在北美设有工厂的公司. 欧洲和亚洲正在设计新的分布式应用程序, 以优化其全球供应链和制造流程. 在一个大洲上预订的订单应该在一秒钟或更短的时间内对所有地区都可见. 数据库应该能够以较短的恢复时间目标 (RTO) 支持故障转移. 应用程序的正常运行时间对于确保不影响生产非常重要.

解决方案架构师应该建议什么?

- A. 使用 Amazon DynamoDB 全局表
- B. 使用 Amazon Aurora 全局数据库
- C. 将 Amazon RDS for MySQL 与跨区域只读副本一起使用
- D. 将 Amazon RDS for PostgreSQL 与跨区域只读副本一起使用

答案:A

**Q300.** 一家公司出于安全原因在私有子网中设置了多个 Amazon EC2 实例. 这些实例托管着定期在 Amazon S3 上读取和写入大量数据的应用程序.

当前, 子网路由通过 NAT 网关定向发往 Internet 的所有流量. 该公司希望在不影响应用程序与 Amazon S3 或外部互联网通信的能力的情况下优化总体成本.

解决方案架构师应采取什么措施来优化成本?

- A. 创建另一个 NAT 网关更新路由表以路由到 NAT 网关.  
更新网络 ACL 以允许 S3 流量
- B. 创建一个 Internet 网关更新路由表以将流量路由到 Internet 网关.  
更新网络 ACL 以允许 S3 通信.
- C. 为 Amazon S3 创建 VPC 终端节点将终端节点策略附加到终端节点.  
更新路由表以将流量定向到 VPC 端点
- D. 在 VPC 外部创建一个 AWS Lambda 函数以处理 S3 请求.  
将 IAM 策略附加到 EC2 实例, 允许它们调用 Lambda 函数.

答案:C

**Q301.** 一家公司在一系列 Amazon EC2 实例上托管一个培训站点. 该公司预计, 其新课程将在一周内发布, 将非常受欢迎, 该课程由网站上的数十个培训视频组成. 解决方案架构师应该怎么做才能最大程度地减少预期的服务器负载?

- A. 将视频存储在 Amazon ElastiCache for Redis 中.  
使用 Elasticache API 更新 Web 服务器以提供视频
- B. 将视频存储在 Amazon Elastic File System (Amazon EFS) 中.  
为 Web 服务器创建用户数据脚本以挂载 EFS 卷.
- C. 将视频存储在 Amazon S3 存储桶中.  
创建具有该 S3 存储桶的原始访问身份 (OAI) 的 Amazon CloudFront 分配.  
限制 Amazon S3 对 OAI 的访问.
- D. 将视频存储在 Amazon S3 存储桶中.  
创建一个 AWS Storage Gateway 文件网关以访问 S3 存储桶.  
为 Web 服务器创建用户数据脚本以安装文件网关

答案:C



淘宝：国际认证大师 微信：ANYPASS

**Q302.** 一家媒体公司将视频内容存储在 Amazon Elastic Block Store (Amazon EBS) 卷中. 某个视频文件已变得很流行，世界各地的大量用户正在访问此内容. 这导致成本增加.

在不影响用户可访问性的情况下，减少费用的措施是什么？

- A. 将 EBS 卷更改为 Provisioned IOPS (PIOPS) .
- B. 将视频存储在 Amazon S3 存储桶中并创建 Amazon CloudFront 发行版.
- C. 将视频分成多个较小的段，以便仅将用户路由到请求的视频段.
- D. 清除每个区域中的 Amazon S3 存储桶并上传视频，以便将用户路由到最近的 S3 存储桶.

答案：B

**Q303.** 解决方案架构师正在为部署到 AWS 的新应用程序设计云架构. 该应用程序允许用户以交互方式下载和上传文件. 超过 2 年的文件将不那么频繁地访问. 解决方案架构师需要确保应用程序可以扩展到任意数量的文件，同时保持高可用性和持久性.

解决方案架构师应该推荐哪些可扩展解决方案？（选择两个.）

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- A. 使用生命周期策略将文件存储在 Amazon S3 上，该策略将 2 年以上的对象移动到 S3 Glacier.
- B. 使用生命周期策略将文件存储在 Amazon S3 上，该策略将 2 年以上的对象移动到 S3 Standard-Infrequent Access (S3 Standard-IA)
- C. 使用生命周期策略将文件存储在 Amazon Elastic File System (Amazon EFS) 上，该策略将 2 年以上的对象移动到 EFS 不频繁访问 (EFS IA).
- D. 将文件存储在 Amazon Elastic Block Store (Amazon EBS) 卷中。计划卷的快照。使用快照可以存档 2 年以上数据。
- E. 将文件存储在 RAID 分割的 Amazon Elastic Block Store (Amazon EBS) 卷中。计划卷的快照。使用快照可以存档 2 年以上数据。

答案：BC

**Q304.** 一家公司在其注册的母域下托管着多个业务类别的多个网站。访问这些网站的用户将基于子域被路由到适当的后端 Amazon EC2 实例。这些网站托管静态网页，图像以及服务器端脚本，例如 PHP 和 JavaScript.

有些网站在营业的前两个小时内访问高峰，并且在一天中的其余时间中不断使用。解决方案架构师需要设计一种解决方案，该解决方案将自动调整这些流量模式的容量，同时保持较低的成本。

哪种 AWS 服务或功能组合可以满足这些要求？（选择两个。）

- A. AWS 批处理
- B. 网络负载平衡器
- C. 应用程序负载平衡器
- D. Amazon EC2 自动扩展
- E. Amazon S3 网站托管

答案：DE

**Q305.** 解决方案架构师正在创建一个将处理批处理大量数据的应用程序。输入数据将保存在 Amazon S3 中，输出数据将存储在其他 S3 存储桶中。为了进行处理，该应用程序将通过网络在多个 Amazon EC2 实例之间传输数据。

解决方案架构师应采取什么措施来降低总体数据传输成本？

- A. 将所有 EC2 实例放入 Auto Scaling 组。
- B. 将所有 EC2 实例放置在同一 AWS 区域中。
- C. 将所有 EC2 实例放置在同一可用区中。
- D. 将所有 EC2 实例放置在多个可用区中的专用子网中。

答案：C

**Q306.** 一家公司正在 AWS 上为全球用户托管一个选举报告网站。该网站使用带有应用程序负载平衡器的 Auto Scaling 组中的 Web 和应用程序层使用 Amazon EC2 实例。数据库层使用 Amazon

RDS for MySQL 数据库. 该网站每小时都会更新一次选举结果，并且在历史上已经观察到数百名访问报告的用户.

由于不同国家即将举行的选举，该公司预计需求将大大增加。解决方案架构师必须提高网站处理额外需求的能力，同时最大程度地减少对额外 EC2 实例的需求。

哪种解决方案可以满足这些要求？

- A. 启动 Amazon ElastiCache 集群以缓存常见的数据库查询。
- B. 启动 Amazon CloudFront Web 分发以缓存常用的网站内容。
- C. 在 EC2 实例上启用基于磁盘的缓存，以缓存通常请求的网站内容。
- D. 使用 EC2 实例将反向代理部署到设计中，并为常用的网站内容启用缓存。

答案：B

**Q307.** 一家公司正在运行一个三层 Web 应用程序来处理信用卡付款。前端用户界面由静态网页组成。应用程序层可以具有长时间运行的进程。

数据库层使用 MySQL。

该应用程序当前在单个通用大型 Amazon EC2 实例上运行。解决方案架构师需要解耦服务，以使 Web 应用程序高度可用。

哪种解决方案将提供最高的可用性？

- 淘宝店名：国际认证大师 微信：ANYPASS
- A. 将静态资产移动到 Amazon CloudFront。  
将应用程序保留在 Auto Scaling 组中的 EC2 中。  
将数据库移至 Amazon RDS 以部署多可用区。
  - B. 将静态资产和应用程序移到中等 EC2 实例中。  
将数据库保留在大型实例上。  
将两个实例都放在一个 Auto Scaling 组中。  
C. 将静态资产移动到 Amazon S3，将应用程序移动到设置了并发限制的 AWS Lambda。  
已启用按需将数据库移动到 Amazon DynamoDB。  
D. 将静态资产移动到 Amazon S3。  
将应用程序移动到启用了 Auto Scaling 的 Amazon Elastic Container Service (Amazon ECS) 容器。  
将数据库移至 Amazon RDS 以部署多可用区。

答案：D

**Q308.** 一家公司在 Amazon EC2 实例上的 Auto Scaling 组中的 Application Load Balancer(ALB) 后面运营一个电子商务网站。该站点正在遇到与 IP 地址不断变化的非法外部系统的高请求率有关的性能问题。安全团队担心对网站的潜在 DDoS 攻击。公司必须以对合法用户影响最小的方式阻止非法的传入请求。

解决方案架构师应该建议什么？

- A. 部署 **Amazon Inspector** 并将其与 ALB 关联.
- B. 部署 AWS WAF, 将其与 ALB 关联, 然后配置速率限制规则.
- C. 将规则部署到与 ALB 关联的网络 ACL 以阻止传入流量.
- D. 部署 **Amazon GuardDuty** 并在配置 GuardDuty 时启用速率限制保护.

答案: B

#### 速率限制

对于基于速率的规则, 请输入在与规则条件匹配的 IP 地址的任何五分钟内允许的最大请求数. 速率限制必须至少为 100.

您可以单独指定速率限制, 也可以指定速率限制和条件. 如果仅指定速率限制, 则 AWS WAF 会将限制应用于所有 IP 地址. 如果您指定速率限制和条件, 则 AWS WAF 将限制限制在符合条件的 IP 地址上.

当 IP 地址达到速率限制阈值时, AWS WAF 通常在 30 秒内尽快应用分配的操作 (阻止或计数). 一旦采取措施, 如果经过五分钟而没有来自 IP 地址的请求, 则 AWS WAF 会将计数器重置为零.  
**Q309.** 一家公司正在为移动应用程序创建一种架构, 该架构需要为其用户提供最小的延迟. 该公司的架构由在 Auto Scaling 组中运行的 Application Load Balancer 后面的 Amazon EC2 实例组成. EC2 实例连接到 Amazon RDS. 应用程序 Beta 测试表明, 读取数据时速度变慢. 但是, 这些指标表明 EC2 实例未超过任何 CPU 使用率阈值.

如何解决这个问题?

淘宝: 国际认证大师 微信: ANYPASS

- A. 降低 Auto Scaling 组中 CPU 利用率的阈值
- B. 用网络负载平衡器替换应用程序负载平衡器
- C. 为 RDS 实例添加只读副本, 并将只读流量定向到该副本
- D. 向 RDS 实例添加多可用区支持, 并将读取流量定向到新的 EC2 实例

答案: C

**Q310.** 一家公司将其静态网站托管在 Amazon S3 存储桶中, 这是 Amazon CloudFront 的起源. 该公司在美国, 加拿大和欧洲都有用户, 并且希望减少用户数量.

解决方案架构师应该建议什么?

- A. 将 CloudFront 缓存生存时间 (TTL) 从默认值调整为更长的时间范围
- B. 使用 Lambda @ edge 实施 CloudFront 事件以运行网站的数据处理
- C. 修改 CloudFront 价格类别以仅包括所服务国家/地区的位置
- D. 实施 CloudFront 安全套接字层 (SSL) 证书以将安全性推向所服务国家/地区的位置

答案: C

**Q311.** 一家媒体公司将视频内容存储在 Amazon Elastic Block Store (Amazon EBS) 卷中. 某些视频文件已变得很流行, 世界各地的大量用户正在访问此内容.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

这导致成本增加.

在不影响用户可访问性的情况下，减少费用的措施是什么？

- A.将 EBS 卷更改为预配置 IOPS (PIOPS)
- B.将视频存储在 Amazon S3 存储桶中并创建和 Amazon CloudFront 发行版
- C.将视频分成多个较小的段，以便仅将用户路由到请求的视频段
- D.在每个区域中创建一个 Amazon S3 存储桶并上传视频，以便将用户路由到最近的 S3 存储桶

答案: B

**Q312.** 一家公司构建了一个新的 VPC，旨在在 AWS 上托管基于 Amazon EC2 的工作负载。解决方案架构师指定创建 Amazon S3 网关终端节点并将其附加到此新 VPC。一旦构建了第一个应用程序服务器，开发人员就会在访问存储在 S3 存储桶中的数据时报告该服务器超时。哪种情况可能导致此问题？（选择两个）

- A. S3 存储桶位于 VPC 以外的区域
- B.端点具有阻止 VPC 的 CIDR 的策略
- C.到 S3 端点的路由未在路由表中配置
- D.访问通过 Internet 网关而不是端点进行路由
- E. S3 存储桶的存储桶策略不允许访问 VPC 的 CIDR

答案: CE

**Q313.** 解决方案架构师正在为 Auto Scaling Web 应用程序设计共享存储解决方案。公司期望对内容进行频繁的更改，因此解决方案必须具有很强的一致性。

哪种解决方案需要最少的努力？

- A.创建一个 Amazon S3 存储桶以存储 Web 内容，并使用 Amazon Cloudfront 交付内容
- B.创建一个 Amazon Elastic File System(Amazon EFS)文件系统并将其安装在单个 Amazon EC2 实例上
- C.创建一个共享的 Amazon Elastic Block 存储(Amazon EBS)卷并将其安装在单个 Amazon EC2 实例上
- D.使用 AWS Datasync 在自动扩展组中的 Amazon EC2 主机之间执行数据的连续同步.

答案: B

**Q314.** 解决方案架构师创建一个将处理批处理大量数据的应用程序。输入数据将保存在 Amazon S3 中，输出数据将存储在其他 S3 存储桶中。为了进行处理，该应用程序将在多个 Amazon EC2 实例之间通过网络传输数据。

解决方案架构师应采取什么措施来降低总体数据传输成本？

- A.将所有 EC2 实例放置在自动缩放组中.
- B.将所有 EC2 实例放置在同一 AWS 区域中

- C. 将所有 EC2 实例放置在同一可用区中
- D. 将所有 EC2 实例放置在多个可用区中的专用子网中

答案: B

**Q315.** 一家公司以前将其数据仓库解决方案迁移到了 AWS. 该公司还拥有一个 AWS Direct Connect 连接公司办公室用户, 可以使用虚拟化工具查询数据仓库. 数据仓库返回的查询的平均大小为 50 MB, 可视化工具发送的每个网页大约为 500 KB. 数据仓库返回的结果集不会被缓存. 哪种解决方案为公司提供了最低的数据传输成本?

- A. 在内部托管可视化工具, 并直接通过 Internet 查询数据仓库.
- B. 将可视化工具托管在与数据仓库相同的 AWS 区域中. 通过互联网访问它.
- C. 在内部托管可视化工具, 并通过 Direct Connect 连接直接在同一 AWS 区域中的某个位置查询数据仓库.
- D. 将可视化工具托管在与数据仓库相同的 AWS 区域中, 并通过 Direct Connect 连接在同一 AWS 区域中的某个位置进行访问.

答案: D

**Q316.** 公司向其用户提供 API, 该 API 可根据商品价格自动进行税款查询. 该公司在假期期间会遇到大量咨询, 但只会导致响应时间变慢. 解决方案架构师需要设计一个可扩展且具有弹性的解决方案.

解决方案架构师应该怎么做才能做到这一点?

淘宝: 国际认证大师 微信: ANYPASS

- A. 提供托管在 Amazon EC2 实例上的 API.  
发出 API 请求时, EC2 实例执行所需的计算.
- B. 使用接受商品名称的 Amazon API Gateway 设计一个 REST API, API Gateway 将商品名称传递给 AWS Lambda 进行税收计算.
- C. 创建一个具有两个 Amazon EC2 实例后面的应用程序负载均衡器.  
EC2 实例将对收到的商品名称计算税额.
- D. 使用 Amazon API Gateway 设计一个 REST API, 该 API 与 Amazon EC2 实例上托管的 API 连接, API Gateway 接受项目名称并将其传递给 EC2 实例以进行税收计算.

答案: B

**Q317.** 公司使用遗留的本地分析应用程序, 该应用程序以.csv 的千兆字节运行, 代表数月的数据. 旧版应用程序可以处理不断增长的.csv 文件. 每天都会从各种数据源向中央本地存储位置添加新的 CSV 文件. 该公司希望在用户学习 AWS 分析服务的同时继续支持旧版应用程序. 为了实现这一目标, 解决方案架构师希望在本地和 Amazon S3 中维护所有.csv 文件的两个同步副本.

解决方案架构师应建议哪种解决方案?

- A. 在本地部署 AWS Datasync.configure Datasync, 以在公司的 S3 存储桶之间连续复制.csv 文件.
- B. 部署本地文件网关, 配置数据源以将.csv 文件写入文件网关, 将旧版分析应用程序指向文件网关.

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

- 文件 gaeway 应该将.csv 文件复制到 Amazon S3.
- C. 部署本地卷网关. 配置数据源以将.csv 文件写入卷网关. 将旧版分析应用程序指向卷网关. 卷网关应将数据复制到 Amazon S3.
- D. 在本地部署 AWS datasync. 配置数据同步以在本地和 Amazon Elastic File System (Amazon EFS) 之间连续复制.csv 文件, 从而支持从 Amazon EFS 复制到公司的 S3 存储桶.

答案: A

**Q318.** 管理层已决定部署所有启用了 IPv6 的 AWS VPC. 一段时间后, 解决方案架构师尝试启动新实例, 并收到一条错误消息, 指出子网中没有足够的 IP 地址空间.

解决方案架构师应该怎么做才能解决此问题?

- A. 检查以确保在 VPC 创建期间仅使用了 IPv6
- B. 创建一个更大范围的新 IPv4 子网, 然后启动实例
- C. 创建一个新的具有更大范围的纯 IPv6 子网, 然后启动实例
- D. 禁用 IPv4 子网, 并将所有实例仅迁移到 IPv6. 完成后, 启动实例.

答案: B

**Q319.** 一家公司正在 AWS 中开发新的机器学习模型解决方案. 这些模型是作为独立的微服务开发的, 可在启动时从 Amazon S3 提取约 1 GB 的模型数据, 并将数据加载到内存中. 用户通过异步 API 访问模型. 用户可以发送一个请求或一批请求, 并指定将结果发送到何处. 公司提供了数百个用户的模型. 模型的使用模式是不规则的. 有些型号可能会在几天或几周内不使用. 其他模型可以一次接收成千上万的请求.

哪种解决方案满足这些要求?

- A. 来自 API 的请求被发送到应用程序负载平衡器(ALB). 模型被部署为 ALB 调用的 AWS Lambda 函数
- B. 来自 API 的请求被发送到模型 Amazon Simple Queue Service (Amazon SOS) 队列. 将模型部署为由 SOS 事件触发的 AWS Lambda 函数. 在 Lambda 上启用了 AWS 自动缩放功能, 以根据 SQS 队列大小增加 vCPUS 的数量.
- C. 来自 API 的请求被发送到模型的 Amazon 简单队列服务 (Amazon SQS) 队列. 模型被部署为从队列读取的 Amazon Elastic Container Service (Amazon ECS) 服务.
- AWS App Mesh** 根据 SQS 队列大小扩展 ECS 集群的实例.
- D. 来自 API 的请求被发送到模型的 Amazon 简单队列服务 (Amazon SQS) 队列. 模型被部署为从队列读取的 Amazon Elastics 容器服务 (Amazon ECS) 服务. 群集均启用了 AWS Auto Scaling ECS, 并根据队列大小复制了服务.

答案: D

**Q320.** 一家公司拥有一个移动游戏, 该游戏从 Amazon RDS 数据库实例读取其大部分元数据. 随着游戏受欢迎程度的提高, 开发人员注意到与游戏元数据加载时间有关的速度降低. 性能指标表明仅扩展数据库将无济于事. 解决方案设计师必须探索所有选项, 包括快照, 复制和亚毫秒级响应时间的功能.

解决方案架构师应建议什么来解决问题？

- A. 使用 Aurora 副本将数据库迁移到 Amazon Aurora.
- B. 使用全局表将数据库迁移到 Amazon DynamoDB.
- C. 在数据库前面添加一个 Amazon ElastiCache for Redis 层.
- D. 在数据库前面添加一个 Amazon ElastiCache for Memcached 层.

答案: C

**Q321** 一家公司运行并使用多个 Amazon EC2 实例从其用户收集数据的应用程序。然后，数据将被处理并传输到 Amazon S3 进行长期存储。对该应用程序的审查显示，很长一段时间没有使用 EC2 实例。解决方案架构师需要设计一种解决方案，以优化利用率并降低成本。

哪种解决方案满足这些要求？

- A. 在按需实例的 Auto Scaling 组中使用 Amazon EC2.
- B. 构建应用程序以将 Amazon Lightsail 与按需实例一起使用.
- C. 创建一个 Amazon CloudWatch cron 作业以在没有活动时自动停止 EC2 实例.
- D. 重新设计应用程序，以将事件驱动的设计与 Amazon Simple Queue Service (Amazon SQS) 和 AWS Lambda 一起使用.

答案: D

**Q322.** 解决方案架构师正在设计带有公共和私有子网的 VPC。VPC 和子网使用 IP 4 CIDR 块。三个可用性区域 (AZ) 中的每一个都有一个公共子网和一个私有子网以实现高可用性。Internet 网关用于为公共子网提供 Internet 访问。专用子网需要访问互联网，以允许 Amazon EC2 实例下载软件更新。

解决方案架构师应该怎么做才能为私有子网启用 Internet 访问？

- A. 创建三个 NAT 网关，每个 AZ 中的每个公共子网一个。  
为每个将非 VPC 流量转发到其 AZ 中的 NAT 网关的 AZ 创建一个专用路由表.
- B. 创建三个 NAT 网关，每个 AZ 中的每个专用子网一个。  
为每个将非 VPC 流量转发到其 AZ 中的 NAT 网关的 AZ 创建一个专用路由表.
- C. 在一个专用子网中创建第二个 Internet 网关。  
为将非 VPC 流量转发到专用 Internet 网关的专用子网更新路由表.
- D. 在一个公共子网中创建一个仅出口的 Internet 网关。  
更新将非 VPC 流量转发到仅出口 Internet 网关的专用子网的路由表.

答案: A

**Q323.** 解决方案架构师需要设计一个网络，该网络将允许多个 Amazon EC2 实例访问用于任务关键型数据的通用数据源，而所有 EC2 实例均可同时访问该数据源。该解决方案必须具有高度的可扩展性，易于实现并支持 NFS 协议。

哪种解决方案满足这些要求？

- A. 创建一个 Amazon EFS 文件系统.  
在每个可用区中配置安装目标.  
将每个实例附加到适当的安装目标.
- B. 创建另一个 EC2 实例，并将其配置为文件服务器.  
创建允许实例之间进行通信的安全组，并将其应用于其他实例.
- C. 使用适当的权限创建一个 Amazon S3 存储桶.  
在 AWS IAM 中创建一个角色，该角色向 S3 存储桶授予正确的权限.  
将角色附加到需要访问数据的 EC2 实例.
- D. 创建具有适当权限的 Amazon EBS 卷.  
在 AWS IAM 中创建一个角色，该角色向 EBS 卷授予正确的权限.  
然后将角色附加到需要访问数据的 EC2 实例.

答案：A

**Q324** 公司在 Auto Scaling 组中的多个 Amazon EC2 实例上部署了多层应用程序。Amazon RDS for Oracle 实例是使用特定于 Oracle 的 PL/SQL 函数的应用程序数据层，到该应用程序的流量一直在稳定增长。这导致 EC2 实例过载，并且 RDS 实例的存储空间不足。Auto Scaling 组没有任何扩展指标，仅定义了最小运行状况实例数。该公司预测，流量趋于平稳之前将继续以稳定但无法预测的速度增长。

解决方案架构师应该怎么做才能确保系统可以自动扩展以适应增加的流量？（选择两个。）

- 淘宝店名：国际认证大师 微信：ANYPASS
- A. 在 RDS for Oracle 实例上配置存储自动扩展.
  - B. 将数据库迁移到 Amazon Aurora 以使用 Auto Scaling 存储.
  - C. 在 RDS for Oracle 实例上配置警报，以减少可用存储空间.
  - D. 将 Auto Scaling 组配置为使用平均 CPU 作为缩放指标.
  - E. 将 Auto Scaling 组配置为使用平均可用内存作为缩放指标.

答案：AD

**Q325.** 一家公司正准备在 AWS 云中启动面向公众的 Web 应用程序。该架构由位于弹性负载均衡器（ELB）后面的 VPC 中的 Amazon EC2 实例组成。**DNS 使用第三方服务。** 该公司的解决方案架构师必须推荐一种解决方案，以检测和防御大规模 DDoS 攻击。

哪种解决方案满足这些要求？

- A. 在账户上启用 Amazon Guard Duty
- B. 在 EC2 实例上启用 Amazon Inspector
- C. 启用 AWS Shield 并为其分配 Amazon Route 53.
- D. 启用 AWS Shield Advanced 并将 ELB 分配给它.

答案：D

**Q326.** 一家公司具有从其本地服务器到 AWS 的 10 Gbps AWS Direct Connect 连接。使用连接的工作负载至关重要。该公司需要具有最大弹性的灾难恢复策略，以将当前连接带宽保持在最低水平。

解决方案架构师应该建议什么？

- A. 在另一个 AWS 区域中建立新的 Direct Connect 连接。
- B. 在另一个 AWS 区域中建立一个新的 AWS 托管 VPN 连接。
- C. 在当前的 AWS 区域中建立两个新的 Direct Connect 连接，在另一个区域中建立一个。
- D. 在当前 AWS 区域中设置两个新的 AWS 托管 VPN 连接，在另一个区域中设置一个。

答案: A

**Q327.** 一家公司在 AWS 中存储用户数据。数据在工作时间内连续使用，高峰使用。访问方式各不相同，有些数据一次不能使用几个月。解决方案架构师必须选择一种经济高效的解决方案，该解决方案可以在保持最高可用性的同时保持最高可用性。

哪种存储解决方案满足这些要求？

- A. 亚马逊 S3
- B. Amazon S3 智能分层
- C. Amazon S3 Glacier Deep 存档
- D. Amazon S3 一区不频繁访问 (S3 One Zone-IA)

答案: B 淘宝：国际认证大师 微信：ANYPASS

**Q328.** 公司没有现有的文件共享服务。一个新项目需要访问可作为本地台式机驱动器安装的文件存储。文件服务器必须先对 Active Directory 域进行身份验证，然后才能访问存储。

哪些服务将允许 Active Directory 用户将存储作为驱动器安装在桌面上？

- A. AWS S3 Glacier
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway

答案: B

**Q329.** 一家公司计划将旧版应用程序迁移到 AWS。该应用程序当前使用 NFS 与本地存储解决方案进行通信以存储应用程序数据。为此，不能将应用程序修改为使用 NFS 以外的任何其他通信协议。

解决方案架构师应建议在迁移后使用哪种存储解决方案？

- A. AWS DataSync
- B. Amazon Elastic Block Store (Amazon EBS)

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

- C.Amazon 弹性文件系统 (Amazon EFS)
- D.Amazon EMR 文件系统 (Amazon EMRFS)

答案: A

**Q330.** 一家公司在两个 Amazon EC2 实例上托管了一个动态 Web 应用程序. 该公司拥有自己的 SSL 证书, 该证书在每个实例上执行 SSL 终止.

最近流量增加了, 运营团队确定 SSL 加密和解密正在使 Web 服务器的计算能力达到其最大限制.

解决方案架构师应该怎么做才能提高应用程序的性能?

- A. 使用 AWS Certificate Manager (ACM) 创建新的 SSL 证书.  
在每个实例上安装 ACM 证书.
- B. 创建一个 Amazon S3 存储桶将 SSL 证书迁移到 S3 存储桶.  
配置 EC2 实例以引用存储桶以终止 SSL.
- C. 创建另一个 EC2 实例作为代理服务器.  
将 SSL 证书迁移到新实例, 并将其配置为将连接定向到现有 EC2 实例.
- D. 将 SSL 证书导入 AWS Certificate Manager (ACM).  
使用使用来自 ACM 的 SSL 证书的 HTTPS 倾听器创建应用程序负载平衡器.

答案: D

**Q331.** 解决方案架构师正在为一家公司设计安全解决方案, 该公司希望通过 AWS 组织为开发人员提供单独的 AWS 账户, 同时还要保持标准的安全控制. 由于各个开发人员将对他们自己的帐户具有 AWS 帐户根用户级别的访问权限, 因此解决方案架构师希望确保不会修改应用于新开发人员帐户的强制性 AWS CloudTrail 配置.

哪个动作符合这些要求?

- A. 创建一个禁止更改 CloudTrail 的 IAM 策略, 并将其附加到 root 用户.
- B. 在启用了组织跟踪选项的情况下, 从开发人员帐户中的 CloudTrail 中创建新跟踪.
- C. 创建一个禁止更改 CloudTrail 的服务控制策略 (SCP), 并将其附加到开发人员帐户.
- D. 使用策略条件为 CloudTrail 创建服务链接角色, 该策略条件仅允许从主帐户中的 Amazon 资源名称 (ARN) 进行更改.

答案: C

**Q332.** 一家公司正在构建媒体共享应用程序, 并决定使用 Amazon S3 进行存储. 上载媒体文件后, 公司开始执行多个步骤来创建缩略图, 识别图像中的对象, 将视频转码为标准格式和分辨率, 以及提取元数据并将其存储到 Amazon DynamoDB 表中. 元数据用于搜索和导航. 流量是可变的. 该解决方案必须能够在不产生不必要的费用的情况下扩展负载峰值.

解决方案架构师应建议什么来支持此工作负载?

- A. 将处理过程内置到用于将内容上传到 Amazon S3 的网站或移动应用程序中, 然后在上传对象后将所需数据保存到 DynamoDB 表中

- B. 当对象存储在 S3 存储桶中时，触发一个 AWS Lambda 函数。  
让步骤函数执行处理对象所需的步骤，然后将元数据写入 DynamoDB 表。
- C. 当对象存储在 S3 存储桶中时，触发 AWS Lambda 函数。  
让 Lambda 函数启动 AWS 批处理以执行处理对象的步骤。完成后，将对象数据放在 DynamoDB 表中。
- D. 当将对象上传到 Amazon S3 时，触发一个 AWS Lambda 函数在 DynamoDB 表中存储一个初始条目，使用在 Auto Scaling 组中的 Amazon EC2 实例上运行的程序来轮询索引中是否有未处理的项目，然后使用该程序执行处理。

答案：B

**Q333.** 一家公司正准备将其预置型应用程序迁移到 AWS。该应用程序由应用程序服务器和 Microsoft SQL Server 数据库组成。无法将数据库迁移到其他引擎，因为应用程序的 .NET 代码中使用了 SQL Server 功能。该公司希望获得最大的可用性，同时最大程度地减少运营和管理开销。

解决方案架构师应该怎么做才能做到这一点？

- A. 在多可用区部署中的 Amazon C2 上安装 SQL Server。
- B. 在多可用区部署中，将数据迁移到 SQL Server 的 Amazon RDS。
- C. 在具有多可用区副本的 SQL Server 的 Amazon RDS 上部署数据库。
- D. 在跨区域多可用区部署中将数据迁移到 SQL Server 的 Amazon RDS

答案：B

**Q334.** 一家公司正在使用 Site-Site VPN 连接来从内部安全地连接到其 AWS 云资源，由于与 Amazon EC2 实例的 VPN 连接之间的流量增加，用户体验到较慢的 VPN 连接。

哪种解决方案可以提高 VPN 吞吐量？

- A. 为同一网络实现多个客户网关以扩展吞吐量
- B. 使用具有相等成本的多路径路由的 Transit 网关，并添加其他 VPN 隧道。
- C. 用等价的多路径路由和多个通道配置一个虚拟网关。
- D. 增加 VPN 配置中的隧道数量以将吞吐量扩展到默认限制之外。

答案：A

**Q335.** 一家移动游戏公司在 Amazon EC2 实例上运行复制服务器。服务器每 15 分钟从玩家那里收到一次更新。该移动游戏会创建一个自上次更新以来在游戏中取得的进展的 JSON 对象，然后将该 JSON 对象发送给 Application Load Balancer。在玩手机游戏时，游戏更新丢失了。该公司希望创建一种持久的方式来按顺序获取更新。

解决方案架构师应该建议采取什么措施来解耦系统？

- A. 使用 Amazon Kinesis Data Streams 捕获数据并将 JSON 对象存储在 Amazon S3 中。
- B. 使用 Amazon Kinesis Data Firehouse 捕获数据并将 JSON 对象存储在 Amazon S3 中

- C. 使用 Amazon 简单队列服务 (Amazon SQS) FIFO 队列捕获数据，并使用 EC2 实例处理队列中的消息。
- D. 使用 Amazon 简单通知服务 (Amazon SNS) 捕获数据，并使用 EC2 实例处理发送到应用程序负载均衡器的消息。

答案: C

**Q336.** 最近创建的一家初创公司构建了一个三层 Web 应用程序。前端具有静态内容。应用层基于微服务。用户数据存储为 JSON 文档，需要以低延迟进行访问。该公司预计第一年的常规流量会很低，每个月发布新功能时流量会达到峰值。启动团队需要将运营开销成本降至最低。

解决方案架构师应该推荐什么来实现这一目标？

- A. 使用 Amazon S3 静态网站托管来存储和服务前端。  
将 AWS Elastic Beanstalk 用于应用程序层。  
使用 Amazon DynamoDB 存储用户数据。
- B. 使用 Amazon S3 静态网站托管来存储和服务前端。  
将 Amazon Elastic Kubernetes 服务 (Amazon EKS) 用于应用程序层。  
使用 Amazon DynamoDB 存储用户数据。
- C. 使用 Amazon S3 静态网站托管来存储和服务前端。  
将 Amazon API Gateway 和 Lambda 函数用于应用程序层。  
使用 Amazon DynamoDB 存储用户数据。
- D. 使用 Amazon S3 静态网站托管来存储和服务前端。  
将 Amazon API Gateway 和 Lambda 函数用于应用程序层。  
将 Amazon RDS 与只读副本一起使用以存储用户数据。

答案: C

**Q337.** 公司需要遵守一项法规要求，该要求规定所有电子邮件必须在外部存储和存档 7 年。管理员已在本地创建了压缩的电子邮件文件，并希望通过托管服务将文件传输到 AWS 存储。

解决方案架构师应建议哪种托管服务？

- A. Amazon 弹性文件系统 (Amazon EFS)。
- B. 亚马逊 S3 冰川。
- C. AWS 备份。
- D. AWS 存储网关。

答案: D

**Q338.** Acompany 的近实时流应用程序正在 AWS 上运行。提取数据后，将在 30 分钟内完成对数据和故事的作业。由于大量传入数据，工作负载经常遇到高延迟。解决方案架构师需要设计可扩展的无服务器解决方案以提高性能。

解决方案架构师应采取哪些步骤组合？（选择两个）

- A. 使用 Amazon Kinesis Data Firehose 提取数据.
- B. 将 AWS Lambda 与 AWS Step Functions 结合使用来处理数据.
- C. 使用 AWS Database Migration Service (AWS DMS) 提取数据.
- D. 在 Auto Scaling 组中使用 Amazon EC2 实例来处理数据.
- E. 将 AWS Fargate 与 Amazon Elastic Container Service (Amazon ECS) 结合使用来处理数据.

答案: AB

Q339. 一家公司计划将多个 TB 的数据传输到 AWS. 数据是从船上离线收集的. 该公司希望在传输数据之前进行复杂的转换.

解决方案架构师应为此迁移推荐哪种 AWS 服务?

- A. AWS Snowball.
- B. AWS Snowmobile.
- C. 优化的 AWS Snowball Edge 存储.
- D. 优化 AWS Snowball Edge 计算.

答案: D

Q340. 公司在其网站上维护可搜索的项目存储库. 数据存储在 Amazon RDS for MySQL 数据库表中, 该表包含超过 1000 万行. 该数据库具有 2 TB 的通用 SSD (gp2) 存储. 每天通过公司网站都有数以百万计的对此数据进行更新. 该公司已注意到某些操作需要 10 秒钟或更长时间, 并且已确定数据库存储性能是瓶颈.

淘宝: 国际认证大师 微信: ANYPASS

哪种解决方案可以解决性能问题?

- A. 将存储类型更改为 Provisioned IOPS SSD (io1).
- B. 将实例更改为内存优化的实例类.
- C. 将实例更改为可爆发的性能数据库实例类.
- D. 使用 MySQL native 异步复制启用 Multi-AZ RDS 只读副本.

答案: A

Q341. 一家公司的混合应用程序托管在具有静态 IP 地址的多个本地服务器上. 已经存在一个 VPN, 可以在 VPC 和内部网络之间提供连接. 该公司希望在本地服务器上为 Internet 用户分配 TCP 流量.

解决方案架构师应建议什么以提供高度可用且可扩展的解决方案?

- A. 启动一个面向互联网的网络负载平衡器 (NLB), 并向 NLB 注册本地 IP 地址.
- B. 启动面向 Internet 的应用程序负载平衡器 (ALB), 并向 ALB 注册本地 IP 地址.
- C. 启动一个 Amazon EC2 实例, 附加一个弹性 IP 地址, 并将流量分配到本地服务器.
- D. Auto Scaling 组中的启动和 Amazon EC2 实例都有公共 IP 地址, 将流量分配到本地服务器.

答案: A

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

**Q342.** 一家公司没有可以生成大量文件的应用程序，每个文件的大小约为 5 MB。文件存储在 Amazon S3 中。公司政策要求文件必须保存 4 年，然后才能删除。始终需要立即可访问性，因为文件包含不容易复制的关键业务数据。在创建对象的前 30 天中经常访问文件，但在前 30 天后很少访问文件。

哪种存储解决方案最符合成本效益？

- A. 创建一个 S3 存储桶生命周期策略，以在对象创建 30 天后将文件从 S3 Standard 迁移到 S3 Glacier。  
创建对象 4 年后删除文件。
- B. 创建一个 S3 存储桶生命周期策略，以在对象创建后 30 天之内将文件从 S3 Standard 迁移到 S3 One Zone-Infrequent Access (S3 One Zone-IA)。  
创建对象 4 年后删除文件。
- C. 创建一个 S3 存储桶生命周期策略，以在对象创建 30 天后将文件从 S3 Standard 迁移到 S3 Standard-Infrequent Access (S3 Standard-IA)。  
创建对象 4 年后删除文件。
- D. 创建一个 S3 存储桶生命周期策略，以在对象创建 30 天后将文件从 S3 Standard 移动到 S3 Standard-Infrequent Access (S3 Standard-IA)。  
创建对象 4 年后，将文件移动到 S3 Glacier。

答案: C

**Q343.** 在线购物应用程序访问 Amazon RDS Multi-AZ 数据库实例。数据库性能正在减慢应用程序的速度。升级到下一代实例类型后，性能没有明显改善。

分析显示，大约有 700 IOPS 的持续性，常见查询可以长时间运行，并且内存利用率很高。

解决方案架构师应建议哪种应用程序更改来解决这些问题？

- A. 将 RDS 实例迁移到 Amazon Redshift 集群并启用每周垃圾收集。
- B. 将长期运行的查询插入新的 Multi-AZ RDS 数据库，并修改应用程序以仅在需要时查询哪个数据库。
- C. 部署两个节点的 Amazon ElastiCache 集群，并修改应用程序以仅在需要时查询哪个数据库。
- D. 为常见查询创建一个 Amazon Simple Queue Service (Amazon SQS) FIFO 队列，并首先对其进行查询，仅在需要时查询数据库

答案: C

**Q344.** 一家公司使用服务器 Amazon EC2 实例将其 Web 应用程序托管在 AWS 上。该公司要求对所有正常 EC2 实例的 IP 地址进行重新编码以响应 DNS 查询。

应该使用哪个策略来满足此要求？

- A. 简单的路由策略。
- B. 延迟路由策略。

- C. 多值路由策略.
- D. 地理位置路由策略.

答案: C

**Q345.** 作为预算计划的一部分, 管理层希望获得用户列出的 AWS 计费项目的报告. 该数据将用于创建部门预算. 解决方案架构师需要确定获取此报告信息的最有效方法.

哪种解决方案满足这些要求?

- A. 使用 Amazon Athena 运行查询以生成报告.
- B. 在 Cost Explorer 中创建一个报告并下载该报告.
- C. 从结算信息中心访问账单详细信息并下载账单.
- D. 修改 AWS 预算中的成本预算并通过 Amazon Simple Email Service (Amazon SES) 发出警报.

答案: B

**Q346.** 一家公司正在准备将机密数据存储在 Amazon S3 中. 出于合规性原因, 必须静态加密数据. 必须记录加密密钥的使用情况以进行审核. 钥匙必须每年旋转一次.

哪种解决方案符合这些要求, 并且在运营上最有效?

- A. 使用客户提供的密钥 (SSE-C) 进行服务器端加密
- B. 使用 Amazon S3 托管密钥 (SSE-S3) 进行服务器端加密
- C. 使用 AWS KMS (SSE-KMS) 客户主密钥 (CMK) 手动旋转服务器端加密.
- D. 使用自动旋转的 AWS KMS (SSE-KMS) 客户主密钥 (CMK) 进行服务器端加密.

答案: D

**Q347.** 一家公司在其数据中心的网络连接存储 (NAS) 中存储了 700 TB 的备份数据. 对于很少的法规要求, 必须可以访问此备份数据, 并且必须保留 7 年. 该公司已决定将此备份数据从其数据中心迁移到 AWS. 迁移必须在 1 个月内完成. 该公司在其公共 Internet 连接上具有 500 Mbps 的专用带宽, 可用于数据传输.

解决方案架构师应该怎么做才能以最低的成本迁移和存储数据?

- A. 订购 AWS Snowball 设备以传输数据.  
使用生命周期策略将文件过渡到 Amazon S3 Glacier Deep Archive.
- B. 在数据中心和 Amazon VPC 之间部署 VPN 连接.  
使用 AWS CLI 将数据从本地复制到 Amazon S3 Glacier.
- C. 提供 500 Mbps 的 AWS Direct Connect 连接, 并将数据传输到 Amazon S3.  
使用生命周期策略将文件传输到 Amazon S3 Glacier Deep Archive.
- D. 使用 AWS DataSync 传输数据并在本地部署 DataSync 代理.  
使用 DataSync 任务将文件从本地 NAS 存储复制到 Amazon S3 Glacier.

答案: A

**Q348** 一家公司希望将其 MySQL 数据库从本地迁移到 AWS. 该公司最近经历了数据库中断，这对业务产生了重大影响。为了确保不再发生这种情况，该公司希望在 AWS 上使用可靠的数据库解决方案，以最大程度地减少数据丢失并将每笔交易存储在至少两个节点上。

哪种解决方案满足这些要求？

- A. 创建一个 Amazon RDS 数据库实例，并同步复制到三个可用区中的三个节点。
- B. 创建一个启用了多可用区功能的 Amazon RDS MySQL 数据库实例，以同步复制数据。
- C. 使用 Multi-AZ 创建一个 Amazon RDS MySQL 数据库实例，并在一个单独的 AWS 区域中创建一个只读副本，以同步复制数据。
- D. 创建并安装了 MySQL 引擎的 Amazon EC2 实例，该实例会触发 AWS Lambda 功能以将数据同步复制到 Amazon RDS MySQL 数据库实例。

答案：B

**Q349.** 在 Amazon EC2 实例上运行的应用程序需要安全地访问 Amazon Elastic File System (Amazon EFS) 文件系统上的文件。EFS 文件是使用静态加密存储的。

哪种在 MOST 中访问文件安全的解决方案？

- A. 挂载 Amazon EFS 时启用 TLS。
- B. 将加密密钥存储在应用程序的代码中。
- C. 挂载 Amazon EFS 时启用 AWS Key 管理服务 (AWS KMS)。
- D. 将加密密钥存储在 Amazon S3 存储桶中，并使用 IAM 角色来授予 EC2 实例访问权限。

答案：C

**Q350.** 一家电子商务网站正在将其 Web 应用程序部署为 Application Load Balancer (ALB) 之后的 Amazon Elastic Container Service (Amazon ECS) 容器实例。在活跃期间，网站会变慢，可用性会降低。解决方案架构师会在存在可用性问题时使用 Amazon CloudWatch 警报接收通知，以便他们可以扩展资源。公司管理层希望使用一种能够自动响应此类事件的解决方案。

哪种解决方案满足这些要求？

- A. 设置 AWS Auto Scaling，以在 ALB 上存在超时时扩展 ECS 服务。设置 AWS Auto Scaling 以在 CPU 或内存预留量过高时扩展 ECS 集群。
- B. 设置 AWS Auto Scaling 以在 ALB CPU 利用率过高时扩展 ECS 服务。
- 设置 AWS Auto Scaling 以在 CPU 或内存预留过高时扩展 ECS 集群。
- C. 设置 AWS Auto Scaling 以在服务的 CPU 使用率过高时扩展 ECS 服务。
- 设置 AWS Auto Scaling 以在 CPU 或内存预留过高时扩展 ECS 集群。
- D. 设置 AWS Auto Scaling 以在 ALB 目标组 CPU 利用率过高时扩展 ECS 服务。设置 AWS Auto Scaling 以在 CPU 或内存预留过高时扩展 ECS 集群。

答案：D

**Q351.** 一家公司正在审查最近将三层应用程序迁移到 VPC 的情况. 安全团队发现, 最低特权原则未应用于应用程序层之间的 Amazon EC2 安全组入口和出口规则.

解决方案架构师应该怎么做才能解决此问题?

- A. 使用实例 ID 作为源或目标创建安全组规则.
- B. 使用安全组 ID 作为源或目标创建安全组规则.
- C. 使用 VPC CIDR 块作为源或目标创建安全组规则.
- D. 使用子网 CIDR 块作为源或目标创建安全组规则.

答案: B

**Q352.** 一家公司正在开发托管在 AWS 上的视频转换应用程序. 该应用程序可用于以下各层: 免费层和付费层. 付费层的用户将首先转换他们的视频, 然后免费层的用户将转换他们的视频.

哪种解决方案符合这些要求, 并且最具成本效益?

- A. 付费层有一个 FIFO 队列, 免费层有一个标准队列
- B. 针对所有文件类型的单个 FIFO Amazon Simple Queue Service (Amazon SQS) 队列.
- C. 针对所有文件类型的单个标准 Amazon Simple Queue Service (Amazon SQS) 队列.
- D. 两个标准的 Amazon Simple Queue Service (Amazon SQS) 队列, 其中一个用于付费层, 一个用于免费层.

答案: A

淘宝: 国际认证大师 微信: ANYPASS

**Q353.** 一家公司正在建立一个网站, 该网站依赖于对 Amazon DynamoDB 数据库的读写. 与网站相关的流量可以预测在工作日的工作时间内达到高峰, 而在一夜之间和周末则下降. 解决方案架构师需要设计一种经济高效的解决方案来处理负载.

解决方案架构师应怎么做才能满足这些要求?

- A. 启用 DynamoDB 加速器 (DAX) 缓存数据.
- B. 为 DynamoDB 数据库启用多可用区复制.
- C. 在创建表时启用 DynamoDB 自动缩放.
- D. 在创建表时启用 DynamoDB 按需容量分配.

答案: C

**Q354.** 一家公司正在准备在 AWS 上部署数据湖. 解决方案架构师必须为 Amazon S3 中的静态数据定义加密策略. 公司的安全政策已阐明.

- 钥匙必须每 90 天旋转一次.
- 必须严格区分关键用户和关键管理员之间的职责.
- 必须能够审核密钥使用情况.

解决方案架构师应该建议什么?

淘宝店名: 国际认证大师 网址: <https://imaws.taobao.com> 微信: ANYPASS

- A. 使用 AWS KMS 托管密钥 (SSE-KMS) 和客户托管的客户主密钥 (CMK) 进行服务器端加密.
- B. 使用带有 AWS 托管客户主密钥 (CMK) 的 AWS KMS 托管密钥 (SSE-KMS) 进行服务器端加密.
- C. 使用带有客户管理的客户主密钥 (CMK) 的 Amazon S3 托管密钥 (SSE-S3) 进行服务器端加密.
- D. 使用 Amazon S3 托管密钥 (SSE-S3) 和 AWS 托管客户主密钥 (CMK) 进行服务器端加密.

答案: A

Q355. 一家公司拥有一个本地应用程序，该应用程序会生成大量对时间敏感的数据，并备份到 Amazon S3. 该应用程序已经增长，并且用户抱怨互联网带宽限制。解决方案架构师需要设计一个长期解决方案，以便既能及时备份到 Amazon S3，又对内部用户的互联网连接影响最小。

哪种解决方案满足这些要求？

- A. 建立 AWS VPN 连接并通过 VPC 网关终端节点代理所有流量
- B. 建立一个新的 AWS Direct Connect 连接，并通过该新连接引导备份流量.
- C. 每天订购 AWS Snowball 设备每天将数据加载到 Snowball 设备上，然后每天将设备返回给 AWS.
- D. 通过 AWS 管理控制台提交支持凭单请求从帐户中删除 S3 服务限制.

答案: B

Q356. 一家公司将 Amazon Redshift 用于其数据仓库。该公司希望在发生任何组件故障时确保其数据的高耐久性。

解决方案架构师应该建议什么？

- A. 启用并发缩放.
- B. 启用跨区域快照.
- C. 增加数据保留期限.
- D. 在多可用区中部署 Amazon Redshift.

答案: B

Q357. 一家公司正在将基于 Linux 的 Web 服务器组迁移到 AWS. Web 服务器必须访问共享文件存储中的文件，才能满足迁移日期的某些内容，因此所做的更改最少。

解决方案架构师应该怎么做才能满足这些要求？

- A. 创建一个可以访问 Web 服务器的 Amazon S3 Standard 存储桶.
- B. 配置一个以 Amazon S3 存储桶为源的 Amazon CloudFront 分发.
- C. 创建一个 Amazon Elastic File System (Amazon EFS) 卷并将其安装在所有 Web 服务器上.
- D. 配置 Amazon Elastic Block Store (Amazon EBS) 预置的 IOPS SSD (io1) 卷，并将其安装在所有 Web 服务器上.

答案: C

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS

**Q358.** 解决方案架构师正在计划部署新的静态网站. 该解决方案必须最小化成本, 并提供至少 99% 的可用性.

哪种解决方案满足这些要求?

- A. 将应用程序部署到一个禁用版本控制的 AWS 区域中的 Amazon S3 存储桶.
- B. 将应用程序部署到在两个 AWS 区域和两个可用区中运行的 Amazon EC2 实例.
- C. 将应用程序部署到已启用版本控制和跨区域复制的 Amazon S3 存储桶.
- D. 将应用程序部署到在一个 AWS 区域和一个可用区中运行的 Amazon EC2 实例.

答案: A

**Q359.** 一家公司托管着一个在线购物应用程序, 该应用程序将所有订单存储在 Amazon RDS for PostgreSQL Single-AZ 数据库实例中. 管理层希望消除单点故障, 并已要求解决方案架构师推荐一种在不需更改应用程序代码的情况下最大程度地减少数据库停机时间的方法.

哪种解决方案满足这些要求?

- A. 通过修改数据库实例并指定 Multi-AZ 选项, 将现有数据库实例转换为 Multi-AZ 部署.
- B. 创建一个新的 RDS 多可用区部署.  
拍摄当前 RDS 实例的快照, 并使用快照还原新的多可用区部署.
- C. 在另一个可用区中创建 PostgreSQL 数据库的只读副本.  
使用 Amazon Route 53 加权记录集在数据库之间分配请求.
- D. 将 RDS for PostgreSQL 数据库放置在 Amazon EC2 Auto Scaling 组中, 组的最小大小为 2.  
使用 Amazon Route 53 加权记录集在实例之间分配请求.

答案: A

**Q360.** 一家公司正在使用 Application Load Balancer 在三个 AWS 区域中部署应用程序. Amazon Route 53 将用于在这些区域之间分配流量.

解决方案架构师应使用哪种 Route 53 配置来提供 MOST 高性能体验?

- A. 创建带有延迟策略的 A 记录.
- B. 使用地理位置策略创建 A 记录
- C. 创建具有故障转移策略的 CNAME 记录.
- D. 使用地理邻近策略创建 CNAME 记录.

答案: A

**Q361.** 公司托管用于将文件上传到 Amazon S3 存储桶的应用程序. 上载后, 将对文件进行处理以提取元数据, 该过程不到 5 秒. 上载的数量和频率从每小时几个文件到数百个并发上载不等. 该公司已要求解决方案架构师设计一种符合这些要求的经济高效的体系结构.

解决方案架构师应该建议什么?

- A. 配置 AWS Cloud Trail 路径以记录 S3 API 调用.  
使用 AWS AppSync 来处理文件.
- B. 在 S3 存储桶中配置一个对象创建的事件通知, 以调用 AWS Lambda 函数来处理文件.
- C. 配置 Amazon Kinesis 数据流以处理数据并将数据发送到 Amazon S3.  
调用 AWS Lambda 函数来处理文件.
- D. 配置一个 Amazon Simple Notification Service (Amazon SNS) 主题以处理上传到 Amazon S3 的文件.  
调用 AWS Lambda 函数来处理文件.

答案: B

**Q362.** 公司将数据存储在本地数据中心中, 供多个本地应用程序使用. 该公司希望维护其现有的应用程序环境, 并能够将 AWS 服务用于数据分析和未来的可视化.

解决方案架构师应建议哪种存储服务?

- A. Amazon Redshift.
- B. 用于文件的 AWS Storage Gateway.
- C. Amazon Elastic Block Store (Amazon EBS).
- D. Amazon 弹性文件系统 (Amazon EFS).

答案: A

**Q363.** 一家公司正在开发一种移动游戏, 该游戏将分数更新流式传输到后端处理器, 然后将结果发布在排行榜上. 解决方案架构师需要设计一种解决方案, 该解决方案可以处理大量流量高峰, 按收据顺序处理移动游戏更新, 并将处理后的更新存储在高度可用的数据库中. 该公司还希望最小化维护该解决方案所需的管理开销. 解决方案架构师应怎么做才能满足这些要求?

- A. 将分数更新到 Amazon Kinesis Data Streams.  
使用 AWS Lambda 处理 Kinesis Data Streams 中的更新.  
将已处理的更新存储在 Amazon DynamoDB 中.
- B. 将分数更新推送到 Amazon Kinesis Data Streams.  
使用为 Auto Scaling 设置的 Amazon EC2 实例队列处理更新.  
将已处理的更新存储在 Amazon Redshift 中.
- C. 将分数更新推送到 Amazon Simple Notification Service (Amazon SNS) 主题.  
将 AWS Lambda 函数订阅到 SNS 主题以处理更新.  
将处理后的更新存储在 Amazon EC2 上运行的 SQL 数据库中.
- D. 将分数更新推送到 Amazon Simple Queue Service (Amazon SQS) 队列.  
使用具有自动扩展功能的 Amazon EC2 实例队列来处理 SQS 队列中的更新.  
将已处理的更新存储在 Amazon RDS Multi-AZ 数据库实例中.

答案: A

重点关注的关键字将是高度可用的数据库-DynamoDB 将是排行榜的更好选择.

**Q364.** 一家公司在 AWS 上具有三层环境，该环境从其用户设备中提取传感器数据。流量先流经网络负载平衡器（NLB），然后流至 Web 层的 Amazon EC2 实例，最后流至进行数据库调用的应用程序层的 EC2 实例。

解决方案架构师应采取什么措施来提高传输到 Web 层的数据的安全性？

- A. 配置 TLS 倾听器，并在 NLB 上添加服务器证书。
- B. 配置 AWS Shield Advanced 并在 NLB 上启用 AWS WAF。
- C. 将负载均衡器更改为应用程序负载均衡器，然后将 AWS WAF 附加到它。
- D. 使用 AWS Key Management Service (AWS KMS) 在 EC2 实例上加密 Amazon Elastic Block Store (Amazon EBS) 卷

答案：A

用户-NLB-EC2（网络）+数据库

**Q365.** 一家公司在不同的 AWS 区域中使用应用程序负载平衡器（ALB）。

ALB 接收的流量不一致，全年可能会出现高峰和下降。该公司的网络团队需要允许本地防火墙中 ALB 的 IP 地址来启用连接。

通过最少的配置更改，MOST 可以扩展哪种解决方案？

- A. 编写一个 AWS Lambda 脚本以获取不同区域中 ALB 的 IP 地址。  
更新本地防火墙规则以允许 ALB 的 IP 地址。
- B. 将不同区域中的所有 ALB 迁移到网络负载平衡器（NLB）。  
更新本地防火墙的规则，以允许所有 NLB 的弹性 IP 地址。
- C. 启动 AWS Global Accelerator 在加速器的不同区域中注册 ALB。  
更新本地防火墙的规则，以允许与加速器关联的静态 IP 地址。
- D. 在一个区域中启动网络负载平衡器（NLB）向 NLB 注册不同区域中 ALB 的专用 IP 地址。  
更新本地防火墙的规则，以允许将弹性 IP 地址附加到 NLB。

答案：C

**Q366.** 公司的数据中心提供商的服务不一致，因为该公司的总部位于遭受自然灾害影响的地区。

该公司尚未准备好完全迁移到 AWS Cloud，但希望在 AWS 上建立故障环境，以防本地数据中心发生故障。

该公司运行连接到外部供应商的 Web 服务器。AWS 和内部场所中可用的数据必须统一。

解决方案架构师应建议哪种解决方案停机时间最少？

- A. 配置 Amazon Route 53 故障转移记录。  
在 Auto Scaling 组中 Application Load Balancer 后面的 Amazon EC2 实例上运行应用程序服务器。  
设置具有存储卷的 AWS Storage Gateway，以将数据备份到 Amazon S3。

B. 配置 Amazon Route 53 故障转移记录.

从脚本执行 AWS CloudFormation 模板, 以在 Application Load Balancer 之后创建 Amazon EC2 实例.

设置具有存储卷的 AWS Storage Gateway, 以将数据备份到 Amazon S3.

C. 配置 Amazon Route 53 故障转移记录.

在 VPC 和数据中心之间建立 AWS Direct Connect 连接.

在 Auto Scaling 组中的 Amazon EC2 上运行应用程序服务器.

运行 AWS Lambda 函数以执行 AWS CloudFormation 模板以创建应用程序负载均衡器.

D. 配置一个 Amazon Route 53 故障转移记录.

运行 AWS Lambda 函数以执行 AWS CloudFormation 模板以启动两个 Amazon EC2 实例.

设置具有存储卷的 AWS Storage Gateway, 以将数据备份到 Amazon S3.

在 VPC 和数据中心之间建立 AWS Direct Connect 连接.

答案: B

**Q367.** 一家公司有两个 AWS 账户生产和开发.

开发帐户中准备好代码更改以推送到生产帐户. 在 Alpha 阶段, 开发团队中只有两名高级开发人员需要访问 Production 帐户. 在测试阶段, 更多的开发人员可能还需要访问权限才能执行测试.

解决方案架构师应该建议什么?

A. 在每个帐户中使用 AWS 管理控制台创建两个策略文档.

将策略分配给需要访问权限的开发人员.

B. 在开发帐户中创建 IAM 角色授予一个 IAM 角色对生产帐户的访问权限.

允许开发人员担任该角色.

C. 使用指定开发帐户的信任策略 **在生产帐户中创建 IAM 角色.**

允许开发人员担任该角色.

D. 在生产帐户中创建一个 IAM 组, 并将其添加为指定生产帐户的信任策略中的主体.

将开发人员添加到组中.

答案: C

**Q368.** 一家公司拥有一个带有嵌入式证书的自定义应用程序, 该应用程序可从 Amazon RDS

MySQL 数据库实例管理中检索信息. 该公司表示, 必须以最少的编程工作量来使该应用程序更安全.

解决方案架构师应该怎么做才能满足这些要求?

A. 使用 AWS Key Management Service (AWS KMS) 客户主密钥 (CMK) 创建密钥.

配置应用程序以从 AWS KMS 加载数据库凭证.

启用自动按键旋转.

B. 在 RDS for MySQL 数据库上为应用程序用户创建凭证, 并将凭证存储在 AWS Secrets Manager 中.

配置应用程序以从 Secrets Manager 加载数据库凭据.

创建一个 AWS Lambda 函数, 该函数在 Secret Manager 中轮换凭证.

C. 在 RDS for MySQL 数据库上为应用程序用户创建凭证，并将凭证存储在 AWS Secrets Manager 中。

配置应用程序以从 Secrets Manager 加载数据库凭据。

使用 Secrets Manager 在 RDS for MySQL 数据库中为应用程序用户设置凭据轮换时间表。

D. 在 RDS for MySQL 数据库上为应用程序用户创建凭证，并将凭证存储在 AWS Systems Manager 参数中。

存储将应用程序配置为从参数存储加载数据库凭据。

使用参数存储在 RDS for MySQL 数据库中为应用程序用户设置凭据轮换时间表。

答案: A



Q369. 在 Amazon EC2 实例上运行的应用程序需要访问 Amazon DynamoDB 表 EC2 实例和 DynamoDB 表位于同一 AWS 账户中。解决方案架构师必须配置必要的权限

哪种解决方案将允许从 EC2 实例对 DynamoDB 表的最小特权访问？

A. 使用适当的策略创建一个 IAM 角色，以允许访问 DynamoDB 表。创建实例配置文件以将此 IAM 角色分配给 EC2 实例。

B. 使用适当的策略创建一个 IAM 角色，以允许访问 DynamoDB 表。将 EC2 实例添加到信任关系策略文档中，以使其承担角色。

C. 使用适当的策略创建一个 IAM 用户，以允许访问 DynamoDB 表。将凭证存储在 Amazon S3 存储桶中，并直接从应用程序代码中读取它们。

D. 使用适当的策略创建一个 IAM 用户，以允许访问 DynamoDB 表。确保应用程序将 IAM 凭据安全地存储在本地存储上，并使用它们进行 DynamoDB 调用。

答案:A

FM071828

**Q370.** 一家公司使用 Amazon S3 存储桶为其网站存储静态图像。该公司将权限配置为仅允许特权用户访问 Amazon S3 对象。

解决方案架构师应该怎么做才能防止数据丢失？（选择两个。）

- A. 在 S3 存储桶上启用版本控制。
- B. 在 S3 存储桶上启用访问日志记录。
- C. 在 S3 存储桶上启用服务器端加密。
- D. 配置 S3 生命周期规则以将对象上的 i 传输到 Amazon S3 Glacier。
- E. 使用 MFA 删 除要求多因素身份验证才能删除对象。

答案:AD

FM071836

淘宝：国际认证大师 微信：ANYPASS

淘宝店名：国际认证大师 网址：<https://imaws.taobao.com> 微信：ANYPASS