

1) 一家公司有多 **个 AWS 账户**，这些账户由各个业务部门拥有。其中一个账户最近受到攻击。攻击者启动了大量实例，导致该账户产生很高的账单金额。

该公司解决了安全漏洞，但解决方案架构师需要开发一款解决方案，以防止所有账户过度支出。每个业务部门都希望保留对其 **AWS 账户** 的完全控制权。

解决方案架构师应建议采取哪种解决方案来满足这些要求？

- A) 使用 AWS Organizations。将每个 AWS 账户添加到管理账户。创建一个使用 `ec2:instanceType` 条件键的 SCP，以防止在每个账户中启动高成本实例类型。
- B) 将客户托管的新 IAM 策略附加到每个账户中的 IAM 组。将策略配置为使用 `ec2:instanceType` 条件键来防止启动高成本实例类型。将所有现有 IAM 用户置于每个组中。
- C) 为每个 AWS 账户开启账单提醒。创建 Amazon CloudWatch 告警，以便在账户超过指定支出阈值时随时向账户管理员发送 Amazon Simple Notification Service (Amazon SNS) 通知。
- D) 在每个账户中打开 AWS Cost Explorer。定期查看每个账户的 Cost Explorer 报告，以确保支出不超过预期金额。

2) 一家公司在 AWS Organizations 内的某个组织中拥有多个 AWS 账户。该公司已将其本地部署 Active Directory 与 AWS Single Sign-On (AWS SSO) 集成在一起，以授予 Active Directory 用户跨所有账户管理基础设施的最低权限。

解决方案架构师必须集成需要对所有 AWS 账户拥有只读访问权限的第三方监控解决方案。监控解决方案将在其自己的 AWS 账户中运行。

解决方案架构师应该怎么做才能为监控解决方案提供所需的权限？

- A) 在 AWS SSO 目录中创建一个用户。为该用户分配只读权限集。为该用户分配需要监控的所有 AWS 账户。向第三方监控解决方案提供用户名和密码。
- B) 在组织的管理账户中创建一个 IAM 角色。允许第三方监控解决方案的 AWS 账户代入该角色。
- C) 邀请第三方监控解决方案的 AWS 账户加入组织。启用所有功能。
- D) 创建一个为第三方监控解决方案定义新 IAM 角色的 AWS CloudFormation 模板。在信任策略中指定第三方监控解决方案的 AWS 账户。使用堆栈集跨所有关联的 AWS 账户创建 IAM 角色。

3) 一个团队正在构建一个托管在公共 Amazon S3 存储桶中的 HTML 表单。该表单使用 JavaScript 将数据发布到 Amazon API Gateway API 终端节点。API 终端节点已与 AWS Lambda 函数相集成。该团队已在 API Gateway 控制台中测试了每种方法，并收到了有效响应。

团队必须完成哪些步骤组合，才能使表单成功发布到 API 终端节点并收到有效响应？（请选择两项）

- A) 配置 S3 存储桶以允许跨域资源共享 (CORS)。
- B) 将表单托管在 Amazon EC2 上，而不是在 Amazon S3 上。
- C) 请求增加 API Gateway 的配额。
- D) 在 API Gateway 中启用跨域资源共享 (CORS)。
- E) 配置 S3 存储桶进行 Web 托管。

4) 一家公司运行使用 Amazon API Gateway、AWS Lambda 函数、Amazon Cognito 和 Amazon DynamoDB 的无服务器移动应用程序。在流量激增期间，用户会报告间歇性系统故障。API Gateway API 终端节点正在向有效请求返回 HTTP 状态代码 502（错误网关）错误。

哪种解决方案可以解决此问题？

- A) 增加 Lambda 函数的并发配额。将 Amazon CloudWatch 配置为在 ConcurrentExecutions 指标接近配额时发送通知提醒。
- B) 为 API Gateway API 终端节点上的每秒事务配额配置通知提醒。创建一个 Lambda 函数，该函数将在达到配额时增加配额。
- C) 将用户分片到多个 AWS 地区中的 Amazon Cognito 用户池，以减少用户身份验证延迟。
- D) 使用 DynamoDB 强一致性读取可确保客户端应用程序始终接收最新数据。

5) 一家公司正在 Amazon Elastic Container Service (Amazon ECS) 集群上启动一项新的 Web 服务。该集群由 100 个 Amazon EC2 实例组成。公司策略要求集群实例上的安全组阻止除 HTTPS（端口 443）之外的所有入站流量。

哪种解决方案将满足这些要求？

- A) 使用用户数据脚本将集群实例上的 SSH 端口更改为 2222。通过端口 2222 使用 SSH 登录每个实例。
- B) 使用用户数据脚本将集群实例上的 SSH 端口更改为 2222。使用 AWS Trusted Advisor 通过端口 2222 远程管理集群实例。

- C) 启动没有 SSH 密钥对的集群实例。使用 AWS Systems Manager Run Command 远程管理集群实例。
- D) 启动没有 SSH 密钥对的集群实例。使用 AWS Trusted Advisor 远程管理集群实例。

6) 一家公司有两个 AWS 账户：一个账户用于生产工作负载，另一个账户用于开发工作负载。开发团队和运营团队负责创建和管理这些工作负载。公司需要满足以下要求的安全策略：

- 开发人员需要创建和删除开发应用程序基础设施。
- 操作员需要创建和删除开发和生产应用程序基础设施。
- 开发人员不能拥有生产基础设施的访问权限。
- 所有用户都必须拥有一组 AWS 凭证。

哪种策略将满足这些要求？

A) 在生产账户中：

- 创建可创建和删除应用程序基础设施的运营 IAM 组。
- 为每个操作员创建一个 IAM 用户。将这些用户分配给运营组。

在开发账户中：

- 创建一个可以创建和删除应用程序基础设施的开发 IAM 组。
- 为每个操作员和开发人员创建一个 IAM 用户。将这些用户分配给开发组。

B) 在生产账户中：

- 创建可创建和删除应用程序基础设施的运营 IAM 组。

在开发账户中：

- 创建一个可以创建和删除应用程序基础设施的开发 IAM 组。
- 为每个开发人员创建一个 IAM 用户。将这些用户分配给开发组。
- 为每个操作员创建一个 IAM 用户。将这些用户分配给开发组和生产账户中的运营组。

C) 在开发账户中：

- 创建一个共享 IAM 角色，该角色可以在生产账户中创建和删除应用程序基础设施。
- 创建一个可以创建和删除应用程序基础设施的开发 IAM 组。
- 创建一个可代入共享角色的运营 IAM 组。
- 为每个开发人员创建一个 IAM 用户。将这些用户分配给开发组。
- 为每个操作员创建一个 IAM 用户。将这些用户分配给开发组和运营组。

D) 在生产账户中:

- 创建一个可创建和删除应用程序基础设施的共享 IAM 角色。
- 将开发账户添加到共享角色的信任策略中。

在开发账户中:

- 创建一个可以创建和删除应用程序基础设施的开发 IAM 组。
- 创建一个可代入生产账户中共享角色的运营 IAM 组。
- 为每个开发人员创建一个 IAM 用户。将这些用户分配给开发组。
- 为每个操作员创建一个 IAM 用户。将这些用户分配给开发组和运营组。

7) 解决方案架构师需要降低大数据应用程序的成本。应用程序环境由数百台向 Amazon Kinesis Data Streams 发送事件的设备组成。设备 ID 用作分区键, 因此每台设备都会获得一个单独的分片。每台设备每秒发送 50KB 到 450KB 的数据。AWS Lambda 函数轮询分片、处理数据并将结果存储在 Amazon S3 中。

每小时都会有另一个 Lambda 函数对结果数据运行一个 Amazon Athena 查询, 以识别异常值。此 Lambda 函数可将异常值放入 Amazon Simple Queue Service (Amazon SQS) 队列中。由两个 EC2 实例组成的 Amazon EC2 Auto Scaling 组可监控队列, 并运行 30 秒的流程来解决异常值。这些设备平均每小时提交 10 个异常值。

应用程序的哪种更改组合能够更大限度地降低成本? (请选择两项)

- A) 更改 Auto Scaling 组启动配置, 以使用同一实例系列中的较小实例类型。
- B) 将 Auto Scaling 组替换为消息到达队列时调用的 Lambda 函数。
- C) 重新配置设备和数据流, 以设置 10 个设备对 1 个数据流分片的比率。
- D) 重新配置设备和数据流, 以设置 2 个设备对 1 个数据流分片的比率。
- E) 将所需的 Auto Scaling 组容量更改为单个 EC2 实例。

8) 一家公司在 Application Load Balancer 后面的 Amazon EC2 实例上运行电子商务应用程序。这些实例在跨多个可用区的 Amazon EC2 Auto Scaling 组中运行。成功处理订单后，应用程序立即将订单数据发布到第三方关联应用程序的外部跟踪系统，该系统为订单推荐支付销售佣金。

在成功的营销推广期间，EC2 实例的数量从 2 个增加到 20 个。在此期间，应用程序继续正常工作。但是，请求率的提高使第三方关联应用程序不堪重负，导致请求失败。

解决方案架构师应进行哪种架构更改组合，才能确保整个流程在负载状态下正常运行？（请选择两项）

- A) 将调用关联应用程序的代码移至新的 AWS Lambda 函数。修改应用程序以异步调用 Lambda 函数。
- B) 将调用关联应用程序的代码移至新的 AWS Lambda 函数。修改应用程序以将订单数据放入 Amazon Simple Queue Service (Amazon SQS) 队列中。从队列中调用 Lambda 函数。
- C) 增加新 AWS Lambda 函数的超时时间。
- D) 减少新 AWS Lambda 函数的预留并发数。
- E) 增加新 AWS Lambda 函数的内存。

9) 一家公司在 AWS 上构建了一个在线票务 Web 应用程序。该应用程序托管在 AWS App Runner 上，并使用存储在 Amazon Elastic Container Registry (Amazon ECR) 存储库中的映像。该应用程序会将数据存储在 Amazon Aurora MySQL DB 集群中。该公司已在 Amazon Route 53 中设置了域名。

该公司需要以主动-主动配置跨两个 AWS 地区部署此应用程序。

哪种步骤组合可以满足这些要求，同时对架构的更改最少？（选择三项）

- A) 为 ECR 映像设置到第二个区域的 Cross-Region Replication。
- B) 从第二个区域的 ECR 存储库中创建一个 VPC 终端节点。
- C) 通过向第二个区域添加第二个部署目标来编辑 App Runner 配置。
- D) 将 App Runner 部署到第二个区域。设置 Route 53 基于延迟的路由。
- E) 使用两个所需区域中的 Amazon DynamoDB 全局表来更改数据库。
- F) 使用在第二个区域中启用了写入转发的 Aurora 全局数据库。

10) 一家公司在 AWS 云中部署了一个多层 Web 应用程序。该应用程序由以下层组成：

- 一个基于 Windows 的 Web 层，托管在具有弹性 IP 地址的 Amazon EC2 实例上
- 一个基于 Linux 的应用程序层，托管在 EC2 实例上，这些 EC2 实例在使用基于路径的路由的 Application Load Balancer (ALB) 后面运行
- 一个在 Linux EC2 实例上运行的 MySQL 数据库

所有 EC2 实例都使用基于英特尔的 x86 CPU。解决方案架构师需要对基础设施进行现代化改造以实现更出色的性能。该解决方案必须最大限度地减少应用程序的运营开销。

解决方案架构师应采取哪些操作组合才能满足这些要求？（请选择两项）

- A) 在多个 EC2 实例上运行 MySQL 数据库。
- B) 将 Web 层实例置于 ALB 后面。
- C) 将 MySQL 数据库迁移到 Amazon Aurora Serverless。
- D) 将所有 EC2 实例类型迁移到 Graviton2。
- E) 将应用程序层实例的 ALB 替换为公司管理的负载均衡器。

答案

- 1) C – [账单告警](#)将向公司提供有关超支的提醒，而不会剥夺任何业务部门的控制权。选项 A 和 B 不正确，因为每个业务部门都希望保留对其账户的控制权。这些选项不会阻止启动大量实例。选项 D 是一个手动流程，不会直接提供有关过度支出的提醒。
- 2) D – [AWS CloudFormation StackSets](#) 只需一次操作即可跨多个账户部署 IAM 角色。选项 A 不正确，因为 AWS Single Sign-On (AWS SSO) 提供的凭证是临时的。应用程序将失去权限，必须重新登录。选项 B 将仅授予对管理账户的访问权限。选项 C 不正确，因为当账户加入组织时，该账户将无法获得访问组织中其他账户的权限。
- 3) D、E – [跨域资源共享 \(CORS\)](#) 是一项浏览器安全功能，可限制从浏览器中运行的脚本发起的 HTTP 请求。构建访问托管在不同域或源上的 API 的 Web 应用程序通常需要 CORS。您可以启用 CORS，以允许来自托管在不同域中的 Web 应用程序对您的 API 的请求。
- 例如，如果您的 API 托管在 [https://\[api_id\].execute-api.\[region\].amazonaws.com/](https://[api_id].execute-api.[region].amazonaws.com/) 上，并且您想从托管在 [\[bucketname\].s3.website-\[region\]](#) 上的 Web 应用程序调用您的 API，您的 API 必须支持 CORS。
- 要通过[网站终端节点](#)提供 HTML 表单，需要选项 E。
- 选项 A 不正确，因为必须将 CORS 标头配置为由 API 终端节点的动态响应返回。为 S3 存储桶配置 CORS 无济于事。选项 B 不正确，因为从 Amazon EC2 上运行的 Web 服务器，而不是从 S3 存储桶提供静态网页没有什么优势。选项 C 不正确，因为 API Gateway 对[每个 AWS 区域的默认配额为每秒 10000 个请求](#)。如有必要，您可以增加此配额。
- 4) A – 如果 AWS Lambda 函数超出其并发配额，Amazon API Gateway 将间歇性地返回 [HTTP 状态代码 502 \(错误网关\) 错误](#)。选项 B 不正确，因为在这种情况下，API Gateway 将[为太多请求返回状态代码 429 错误](#)。选项 C 不正确，因为错误发生在调用 API Gateway API 终端节点期间，而不是在身份验证过程中。选项 D 不正确，因为过时的数据不会导致“错误网关”错误。
- 5) C – [AWS Systems Manager Run Command](#) 不需要打开任何入站端口。Run Command 完全通过出站 HTTPS 运行，默认情况下对安全组开放。选项 A 和 B 不正确，因为要求规定唯一应打开的入站端口是 443。选项 D 不正确，因为 AWS Trusted Advisor 不执行此管理函数。
- 6) D – 正确答案符合在您控制的两个账户之间授予跨账户访问权限的[标准准则](#)。选项 A 不符合要求，因为它要求操作员提供两组凭证。选项 B 不正确，因为您无法将 IAM 用户添加到其他账户中的 IAM 组。选项 C 不正确，因为角色无法授予对其他账户中资源的访问权限。共享角色必须与共享角色管理的资源位于同一账户中。

7) B、D – 每小时处理异常值的平均计算时间为 300 秒（10 个事件，每个事件 30 秒）。选项 B 正确，因为使用 [AWS Lambda](#)，您只需为处理异常值所需的少量计算时间付费。尽管选项 A 和 E 可以降低成本，但它们都涉及为一个或多个 Amazon EC2 实例付费，这些实例每小时会闲置 3300 秒。选项 C 和 D 降低了 Kinesis 数据流的分片小时成本。但是，选项 C 不正确，因为数据量将超过单个分片的 [1MB/s 配额](#)。

8) B、D – 在选项 B 中，使用 [Amazon Simple Queue Service \(Amazon SQS\) 队列](#) 将使主应用程序与对关联应用程序的调用分离。此更改将保护主应用程序免受关联应用程序容量减少的影响。此外，失败的请求可以自动返回队列。在选项 D 中，减少[并发调用次数](#)将防止关联应用程序不堪重负。

尽管选项 A 将减少 Amazon EC2 实例的负载，但此解决方案不会减少对关联应用程序的请求数量。尽管选项 C 将允许 AWS Lambda 函数等待更长时间以便让外部调用返回，但此解决方案不会减少不堪重负的关联应用程序的负载。选项 E 不正确，因为内存的增加不会影响 Lambda 函数和关联跟踪系统之间的交互。

9) A、D、F – [AWS App Runner](#) 是一项完全托管的服务，开发人员可以使用它和存储在 Amazon Elastic Container Registry (Amazon ECR) 存储库中的映像快速部署容器化 Web 应用程序。选项 A 正确，因为 [Cross-Region Replication](#) 可在另一个 AWS 区域中创建存储库的副本。选项 D 正确，因为您可以使用 [Route 53](#) 托管自定义域名，并将流量路由到多个 AWS 地区中的资源。选项 F 正确，因为 [Amazon Aurora 全球数据库](#) 跨多个区域扩展，并且专为分布在全球的应用程序而设计。

选项 B 不正确，因为 VPC 终端节点无法提供对存储在不同区域中的映像的访问权限。在选项 C 中，App Runner 中不存在此类配置。尽管选项 E 可行，但与使用 Aurora 全局数据库相比，引入 Amazon DynamoDB 需要对架构进行更多更改。这个问题要求对架构进行最少更改。

10) B、C – 在选项 B 中，通过将 Web 层置于 [Application Load Balancer \(ALB\)](#) 之后，可以提高 Web 层的可用性和可扩展性。ALB 充当客户端的单一联系点，并将传入的应用程序流量分配到 Amazon EC2 实例。选项 C 正确，因为 [Amazon Aurora Serverless](#) 可提供高性能和高可用性，同时降低运营复杂性。

选项 A 不正确，因为额外的 EC2 实例不会最大限度地减少运营开销。托管式服务将是更好的选择。选项 D 不正确，因为应用程序包含 Windows 实例，而这些实例不适用于 Graviton2。选项 E 不正确，因为公司管理的负载均衡器无法最大限度地减少运营开销。