aws training and certification

Solutions Architect Professional (SAP-C01)
Sample Exam Questions
解决方案架构师专业人员（SAP-C01）
试题示例

1) **企业的大量 AWS 账户为独立业务组所有。其中一个帐户最近遭到入侵。攻击者启动了大量实例，导致该帐户的开销很高。**

安全漏洞已得到解决，但管理层已要求解决方案架构师制定解决方案，以防止所有帐户中出现过度开销。每个业务组都希望保留对其 AWS 账户的完全控制。

解决方案架构师应建议哪一种解决方案来满足这些要求？

A. 使用 AWS Organizations 将每个 AWS 账户添加到主账户。创建使用 `ec2:instanceType` 条件键的服务控制策略（SCP），以防止在每个帐户中启动高成本实例类型。
B. 将新的客户管理的 IAM 策略附加至每个帐户中的 IAM 组，该帐户使用 `ec2:instanceType` 条件键以防止启动高成本实例类型。将所有现有的 IAM 用户放在每个组中。
C. 在每个 AWS 账户上启用计费警报。创建 Amazon CloudWatch 警报，每当客户帐户超出支出预算时，该警报都会向帐户管理员发送 Amazon SNS 通知。
D. 在每个账户中启用 AWS Cost Explorer。定期审查每个帐户的 Cost Explorer 报告，以确保支出不超过计划预算。

2) **一家公司拥有多个 AWS 账户。公司已将其本地活动目录（AD）与 AWS SSO 集成，以授予 AD 用户管理所有账户基础结构的最小特权能力。**

解决方案架构师必须集成需要跨所有 AWS 账户进行只读访问的第三方监控解决方案。该监控解决方案将在其自己的 AWS 账户中运行。

如何为监控解决方案授予所需的权限？

A. 在 AWS SSO 目录中创建用户并分配只读权限集。将要监控的所有 AWS 账户分配给新用户。提供具有用户名和密码的第三方监控解决方案。
B. 在组织的主账户中创建 AWS IAM 角色。允许第三方监控解决方案的 AWS 账户担任该角色。
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 AWS CloudFormation 模板，该模板为第三方监控解决方案及信任策略中列出的第三方账户定义新的 AWS IAM 角色。通过使用堆栈集跨所有链接的 AWS 账户创建 IAM 角色。

3) **团队正在构建托管在公共 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 端点。该端点与 AWS Lambda 函数集成。团队已在 API Gateway 控制台中测试了每种方法，并收到了有效的响应。**

为成功发布到 API Gateway 并接收有效响应，必须完成哪些步骤组合？（选择两个。）

A. 配置 S3 存储桶以允许跨源资源共享（CORS）。
B. 在 Amazon EC2 而不是 Amazon S3 上托管表单。
C. 请求增加 API Gateway 的限制。
D. 在 API Gateway 中启用跨源资源共享（CORS）。
E. 为网络托管配置 S3 存储桶。

4) **一家零售公司运行基于 Amazon API Gateway、AWS Lambda、Amazon Cognito 和 Amazon DynamoDB 构建的无服务器移动应用。在节假日流量高峰期间，公司会收到间歇性系统故障的投诉。开发人员发现 API Gateway 端点将 502 Bad Gateway 错误返回至看似有效的请求。**

哪一种方法应该解决此问题？

A. 提高 Lambda 函数的并发限制，并将 Amazon CloudWatch 发送的通知警报配置为在 `ConcurrentExecutions` 指标接近该限制时发送。
B. 为 API Gateway 端点上为每秒的事务限制配置通知警报，并根据需要创建将增加此限制的 Lambda 函数。
C. 将用户分分开到多个区域中的 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，以确保最新数据始终返回到客户端应用程序。

5) **一家网络托管公司已为每个 AWS 区域中的全部用户启用了 Amazon GuardDuty。系统管理员必须创建对高严重性事件的自动响应。**

应该如何做到这一点？

A. 通过触发 AWS Lambda 函数的 VPC Flow Logs 创建规则，该函数以编程方式解决问题。
B. 创建 AWS CloudWatch Events 规则，该规则可触发以编程方式解决问题的 AWS Lambda 函数。
C. 配置 AWS Trusted Advisor 以触发 AWS Lambda 函数，该函数以编程方式解决问题。
D. 配置 AWS CloudTrail 以触发 AWS Lambda 函数，该函数以编程方式解决问题。

6) **一家公司正在 Amazon ECS 群集上启动新的网络服务。公司政策要求群集实例上的安全组阻止除 HTTPS（端口 443）以外的所有入站流量。该群集由 Amazon 100 个 EC2 实例组成。安全工程师负责管理和更新群集实例。安全工程团队规模较小，因此必须尽量减少任何管理工作。**

如何设计服务以满足这些操作要求？

A. 使用用户数据脚本将群集实例上的 SSH 端口更改为 2222。在端口 2222 上使用 SSH 登录到每个实例。
B. 使用用户数据脚本将群集实例上的 SSH 端口更改为 2222。使用 AWS Trusted Advisor 通过端口 2222 远程管理群集实例。

C. 启动无需 SSH 密钥对的群集实例。使用 Amazon EC2 Systems Manager Run Command 远程管理群集实例。
D. 启动无需 SSH 密钥对的群集实例。使用 AWS Trusted Advisor 远程管理群集实例。

7) 一家公司拥有两个 AWS 账户：一个用于生产工作负载，另一个用于开发工作负载。开发和操作团队将创建和管理工作负载。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结构。**
- **操作人员需要创建和删除开发和生产应用程序基础结构。**
- **开发人员不应访问生产基础结构。**
- **所有用户都应拥有一组 AWS 凭据。**

哪些策略满足这些要求？

A. 在开发帐户中：
- 创建具有创建和删除应用程序基础结构的开发 IAM 组。
- 为每个操作人员和开发人员创建一个 IAM 用户，并将他们分配给开发组。

在生产帐户中：
- 创建能够创建和删除应用程序基础结构的操作 IAM 组。
- 为每个操作人员创建一个 IAM 用户，并将他们分配给操作组。

B. 在开发帐户中：
- 创建具有创建和删除应用程序基础结构的开发 IAM 组。
- 为每个开发人员创建一个 IAM 用户，并将他们分配给开发组。
- 为每个操作人员创建一个 IAM 用户，并将他们分配给生产帐户中的开发组和操作组。

在生产帐户中：
- 创建能够创建和删除应用程序基础结构的操作 IAM 组。

C. 在开发帐户中：
- 创建共享 IAM 角色，该角色能够在生产帐户中创建和删除应用程序基础结构。
- 创建具有创建和删除应用程序基础结构的开发 IAM 组。
- 创建能够承担共享角色的操作 IAM 组。
- 为每个开发人员创建一个 IAM 用户，并将他们分配给开发组。
- 为每个操作人员创建一个 IAM 用户，并将他们分配给开发组和操作组。

D. 在开发帐户中：
- 创建具有创建和删除应用程序基础结构的开发 IAM 组。
- 创建能够承担生产帐户中共享角色的操作 IAM 组。
- 为每个开发人员创建一个 IAM 用户，并将他们分配给开发组。
- 为每个操作人员创建一个 IAM 用户，并将他们分配给开发组和操作组。

在生产帐户中：
- 创建具有创建和删除应用程序基础结构的共享 IAM 角色。
- 将开发帐户添加到共享角色的信任策略。

8) **一家公司正在将 Apache Hadoop 群集从其数据中心迁移到 AWS。该群集由 60 台 VMware Linux 虚拟机（VMs）组成。在迁移群集期间，应尽量减少停机时间。**

哪一种流程将最大限度地减少停机时间？

A. 使用 AWS Management Portal for vCenter 将 VMs 作为 Amazon EC2 实例迁移到 AWS。
B. 使用 AWS SMS 将 VMs 作为 AMIs 迁移到 AWS。在 AWS 上启动群集，从迁移的 AMIs 中作为 Amazon EC2 实例启动。
C. 创建 VMs 的 OVA 文件。将 OVA 文件上传到 Amazon S3。使用 VM Import/Export 从 OVA 文件创建 AMIs。在 AWS 上以 Amazon EC2 实例从 AMIs 启动群集。
D. 将 HDFS 数据从 VMs 导出到新的 Amazon Aurora 数据库。在 Amazon EC2 实例上启动新的 Hadoop 群集。将数据从 Aurora 数据库导入新群集上的 HDFS。

9) **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个将事件发送到 Amazon Kinesis Data Streams 的设备组成。使用设备 ID 作为分区键，因此每个设备都会获得单独的分片。每个设备每秒发送 50KB 和 450KB 的数据。分片由 AWS Lambda 函数轮询，该函数处理数据并将结果存储在 Amazon S3 上。**

AWS Lambda 函数每小时针对结果数据运行 Amazon Athena 查询，该查询可识别任何异常值并将其置于 Amazon SQS 队列中。由两个 EC2 实例组成的 Amazon EC2 Auto Scaling 组监控队列并运行一个短进程（大约 30 秒）来解决异常值。设备每小时平均提交 10 个外围值。

哪一种应用程序的变更组合将最大程度地降低成本？（选择两个。）

A. 更改 Auto Scaling 组启动配置以在同一实例系列中使用较小的实例类型。
B. 将 Auto Scaling 组替换为 AWS Lambda 函数，该函数由到达 Amazon SQS 队列的消息触发。
C. 重新配置设备和数据流，将 10 个设备与 1 个数据流分片的比率设置在一起。
D. 重新配置设备和数据流，将 2 个设备与 1 个数据流分片的比率设置在一起。
E. 将 Auto Scaling 组的所需容量更改为单个 EC2 实例。

10) **一家公司在 ELB 应用程序负载平衡器后面的 Amazon EC2 实例上运行电子商务应用程序。实例在跨多个可用区域的 Amazon EC2 Auto Scaling 组中运行。成功处理订单后，应用程序会立即将订单数据发布到外部第三方子公司追踪系统，该系统为订单转介支付销售佣金。在非常成功的营销推广期间，EC2 实例的数量从 2 个增加到 20 个。应用程序继续正常工作，但请求率的增加使第三方子公司不堪重负，导致请求失败。**

哪一种体系结构更改组合可确保整个流程在负载下正常运行？（选择两个。）

A. 将调用子公司的代码移动到新的 AWS Lambda 函数。修改应用程序以异步调用 Lambda 函数。

B. 将调用子公司的代码移动到新的 AWS Lambda 函数。修改应用程序以将订单数据放入 Amazon SQS 队列中。从队列中触发 Lambda 函数。
C. 增加新的 AWS Lambda 函数的超时。
D. 调整新的 AWS Lambda 函数的并发限制。
E. 增加新的 AWS Lambda 函数的内存。

答案

1) C - 计费警报将允许管理层收到关于过度开销的警报，而不会从任何业务组获得控制权。A 和 B 不正确，因为每个业务组都希望保留对其帐户的控制，并且这些解决方案无法防止启动大量实例。D 是一个手动过程，可能需要一段时间才能发现任何未经授权的支出。

2) D - AWS CloudFormation StackSets 可以通过单个操作跨多个账户部署 IAM 角色。A 不正确，因为 AWS SSO 提供的凭据是临时的，因此应用程序将失去权限，必须重新登录。B 仅授予对主帐户的访问权限。C 不正确，因为属于组织的帐户在其他帐户中不接收权限。

3) D、E - （D）必须启用 CORS 以防止浏览器由于相同的源策略而生成错误，这要求动态内容应来自与静态内容相同的域。由于 API Gateway 使用的是格式为 `[restapi-id].execute-api.amazonaws.com` 的域， 因此 S3 存储桶使用`[bucketname].s3.website-[region].amazonaws.com`，因此必须随 API Gateway 响应发送 CORS 标头，浏览器才能放宽限制。（E）需要通过网站端点**提供 HTML 表单**。A 不正确，因为 CORS 标头必须配置为由 API 端点的动态响应返回。为 S3 存储桶配置 CORS 不起作用。（B）不正确，因为从在 EC2 上运行的 Web 服务器与 S3 存储桶中提供服务没有任何优势。（C）不正确，因为 API Gateway 默认每个区域限制为每秒 10000 个请求。如果生产需要，可以增加此限制。

4) A - 如果 Lambda 函数超过并发限制，API Gateway 将间歇性地返回 502 内部服务器错误。（B）不正确，因为在这种情况下，API Gateway 会由于请求太多而返回 429 错误。（C）不正确，因为调用 API Gateway 端点时（而不是身份验证过程中）发生错误。（D）不正确，因为陈旧数据不会导致非法网关错误。

5) B - GuardDuty 调查结果可以发送到 Amazon SNS 话题和 CloudWatch Events。（A）和（D）不正确，因为 VPC Flow Logs 和 AWS CloudTrail 不可以直接触发 AWS Lambda 函数。（C）不正确，因为 Trusted Advisor 是推荐服务，不适合此方案。

6) C - Amazon EC2 Systems Manager Run Command 要求不打开入站端口；它完全通过出站 HTTPS 运行（默认情况下，安全组打开）。（A）和（B）被排除在外，因为要求明确规定，唯一要打开的入站端口是 443。D 被排除，因为 Trusted Advisor 确实执行管理功能。

7) D - 这是唯一有效并满足要求的响应。它遵循的标准准则，在您控制的两个帐户之间授予跨帐户访问权限。（A）需要为操作人员提供两组凭据，这违反了要求。（B）不起作用，因为无法将 IAM 用户添加到其他帐户中的 IAM 组。（C）不起作用，因为角色不能授予对另一个帐户中的资源的访问权限；共享角色必须在具有其管理资源的帐户中。

8) B – AWS SMS 以增量方式上传每个 VM，以便在数据中心群集仍在运行时上传服务器。数据中心群集必须在所有虚拟机最终增量同步之前关闭。（A）和（C）不符合最小化停机时间的要求。从 vCenter 和 VM Import/Export 文档：对于大多数 VM 导入需求，我们建议您使用 AWS SMS。AWS SMS 可自动执行导入过程（减少迁移大型 VM 基础结构的工作量），添加对更改 VM 的增量更新的支持，并将导入的 VM 转换为即用型 AM。（D）不符合最小化停机时间的要求。

9) B、D – 每小时使用的平均计算量约为 300 秒（10 个事件 x 30 秒）。虽然 A 和 E 都会降低成本，但它们都涉及到为一个或多个 EC2 实例每小时闲置 3300 秒或更长时间而付费。B 只需要支付少量的计算时间来处理外围值。（C）和（D）都降低了 Kinesis Data Stream 的分片小时成本，但（C）将不起作用，因为数据量将超过单个分片的 1 MB/s 限制。

10) B、D – 将消息放入队列（B）将使主应用程序与对子公司的调用分离。这不仅可以保护主应用程序免受联盟成员容量降低的影响，而且还允许失败的请求自动返回队列。限制并发执行数（D）将防止使附属应用程序不堪重负。（A）不正确，因为虽然异步调用 Lambda 函数将减少 EC2 实例的负载，但也不会降低对附属应用程序的请求数。（C）不正确，因为虽然允许 Lambda 函数等待外部调用返回的时间更长，但它不会减少附属应用程序上的负载（这仍然会不堪重负）。（E）不正确，因为调整内存不会影响 Lambda 函数和附属应用程序之间的交互。

