

AWS 认证开发运维工程师 - 专业级
AWS Certified DevOps Engineer - Professional
(DOP-C01) 考试样题

- 1) 一家公司在 AWS CodeCommit 中控制其产品的源代码。该公司使用 AWS CodePipeline 为产品创建 CI/CD 管道。该管道必须在 CodeCommit 存储库的主分支发生更改时自动启动。每天都会对应用程序进行更改，因此需要尽可能提高管道的响应能力。

开发运维工程师应该采取哪些操作来满足这些要求？

- A. 配置管道定期检查存储库。在检测到发生更改时启动管道。
 - B. 配置存储库在发生更改时生成 Amazon CloudWatch Events 事件。配置管道在响应事件时启动。
 - C. 配置存储库定期运行 AWS Lambda 函数。函数应检查存储库并在检测到更改时启动管道。
 - D. 配置存储库在发生更改时发布 SNS 通知。将管道订阅到 Amazon SNS 主题。
- 2) 开发团队希望设置 AWS CodeCommit 存储库。开发人员应该可以将更改推送到自己的分支，但不应允许他们将提交或合并拉取请求推送到主分支。此外，当主分支中出现提交或合并时，项目经理需要收到通知。

哪些步骤的组合可以保护主分支并以最短的延迟发送提醒？（选择两项。）

- A. 将拒绝对主分支执行推送提交、合并拉取请求和添加文件操作的 AWS IAM 策略附加到开发人员 IAM 组。
 - B. 将拒绝 IAM 开发人员组成员对主分支执行推送提交、合并拉取请求和添加文件操作的资源策略附加到 CodeCommit 存储库。
 - C. 设置每 15 分钟运行的 AWS Lambda 函数来检查存储库更改并将通知发布到 Amazon SNS 主题。
 - D. 为主分支设置由 CodeCommit Repository State Change 事件触发的 Amazon CloudWatch Events 规则，并添加 Amazon SNS 主题作为目标。
 - E. 配置 AWS CloudTrail 将日志事件发送到 Amazon CloudWatch Logs。定义指标筛选条件来确定存储库事件。创建以 Amazon SNS 主题为目标的 CloudWatch 警报。
- 3) 一家公司使用 AWS CodeBuild 来构建应用程序。公司政策要求对所有构建项目静态加密。对构件的访问必须限于具有承担操作角色权限的 IAM 用户。

如何满足这些要求？

- A. 将 post-build 命令添加到 CodeBuild 生成规范，该命令将构建对象推送到启用 S3 默认加密的 Amazon S3 存储桶。为所有操作设置包含 Deny 语句的 S3 存储桶策略，在 NotPrincipal 部分中引用操作 IAM 角色。
- B. 将 post-build 命令添加到 CodeBuild 生成规范，该命令将构建对象推送到 Amazon S3 存储桶。设置只有在请求包含标头 x-amz-server-side-encryption 时才允许上传到存储桶的存储桶策略。为所有操作添加 Deny 语句，在 NotPrincipal 部分中引用操作 IAM 组。

AWS 认证开发运维工程师 - 专业级
AWS Certified DevOps Engineer - Professional
(DOP-C01) 考试样题

- C. 将 `post-build` 命令添加到 CodeBuild 生成规范, 该命令将构建对象推送到 Amazon S3 存储桶。配置 S3 事件通知以触发 AWS Lambda 函数以获取对象、对其进行加密, 然后将其放回到具有 `encrypted` 标签键和 `true` 标签值的 S3 存储桶中。为所有操作添加包含 `Deny` 语句的 S3 存储桶策略, 在 `NotPrincipal` 部分中引用操作 IAM 组, 并在 `Condition` 部分中引用 `Encrypted` 标签。
- D. 将 `post-build` 命令添加到 CodeBuild 生成规范, 该命令调用 AWS KMS `Encrypt` API, 将构件传递到 AWS KMS, 从而使用指定的客户主密钥 (CMK) 进行加密。将加密的构件推送到 Amazon S3 存储桶, 并设置 IAM 操作组作为 AWS KMS 中该 CMK 的唯一密钥用户。
- 4) 开发运维工程师希望在 AWS 上为应用程序实施蓝/绿部署流程, 并希望能够在环境之间逐渐转移流量。应用程序运行在位于 ELB Application Load Balancer 之后的 Amazon EC2 实例上。实例运行在 EC2 Auto Scaling 组中。数据存储在 Amazon RDS 多可用区数据库实例中。外部 DNS 由 Amazon Route 53 提供。

哪些步骤的组合可以实施蓝/绿部署流程? (选择三项。)

- A. 在同一个 Application Load Balancer 之后创建第二个 Auto Scaling 组。
- B. 创建第二个 Application Load Balancer 和 Auto Scaling 组。
- C. 在 Route 53 中创建指向新环境的第二个别名记录, 并在两个记录之间使用故障转移路由策略。
- D. 在 Route 53 中创建指向新环境的第二个别名记录, 并在两个记录之间使用加权路由策略。
- E. 配置新 EC2 实例以使用相同的 RDS 数据库实例。
- F. 配置新 EC2 实例以使用 RDS 数据库实例的故障转移节点。
- 5) 开发运维工程师编写了一个 AWS Lambda 函数, 在 AWS CloudFormation 模板代码段 (如下所示) 中定义该函数, 并将其存储在 Amazon S3 存储桶中。

```
MyLambdaFunctionV1:
  Type: "AWS::Lambda::Function"
  Properties:
    Handler: "index.handler"
    Role: "arn:aws:iam::515290864834:role/AccountScanner"
    Code:
      S3Bucket: "johndoe-com-lambda-source"
      S3Key: "AccountScanner.zip"
      Runtime: "dotnetcore2.1"
      Timeout: 60
```

CloudFormation 堆栈已创建, 并且 Lambda 函数按预期工作。工程师获得了新版本的函数代码, 希望确保此新版本可在堆栈更新之后立即执行。

哪些部署过程可完成此操作? (选择三项。)

- A. 在 CloudFormation 模板中将 Lambda 函数的逻辑名称从 `MyLambdaFunctionV1` 更新为 `MyLambdaFunctionV2`, 然后执行 CloudFormation 堆栈更新。

AWS 认证开发运维工程师 - 专业级
AWS Certified DevOps Engineer - Professional
(DOP-C01) 考试样题

- B. 在现有 S3 存储桶上启用版本控制。将新代码上传到现有 S3 存储桶。在 CloudFormation 模板中 Lambda 函数的 S3ObjectVersion 属性中指定 S3 对象的版本 ID，然后执行 CloudFormation 堆栈更新。
 - C. 使用 AWS SAM 发布 `sam deploy` 命令到 CloudFormation 模板，执行 Lambda 函数版本更新。
 - D. 更新 CloudFormation 模板中 Lambda 函数的 S3 存储桶属性，指向不同的存储桶位置。将新代码上传到新的 S3 存储桶位置，然后执行 CloudFormation 堆栈更新。
 - E. 更新 CloudFormation 模板中 Lambda 函数的 S3Key 属性，指示 .zip 文件的不同位置和名称。将新代码上传到新的 S3 存储桶，记录 .zip 文件的位置和名称更改，然后执行 CloudFormation 堆栈更新。
 - F. 使用无服务器框架发布 `serverless deploy function -f MyLambdaFunctionV1` 命令，执行对现有 Lambda 函数的更新。
- 6) 开发运维工程师需要为公司实现自动化的安全合规。公司开发了自定义 AWS Config 规则，用来检测不合规的安全配置。在检测到合规性问题时，公司希望自动修复问题，并且希望通过内部安全消息通道通知安全团队。留言板有一个 REST 接口，该接口通过通道发布 HTTPS POST 请求的正文。

哪些步骤的组合能够以最经济高效的方式成功满足这些要求？（选择三项。）

- A. 创建向 Amazon SNS 主题发布配置项更改通知的 Amazon CloudWatch Events 规则。
 - B. 创建向 Amazon SNS 主题发布合规性更改通知的 Amazon CloudWatch Events 规则。
 - C. 配置 AWS Config，将配置项更改通知发布到 Amazon SNS 主题。
 - D. 创建具有与 AWS Config 的 AWS 集成的 Amazon API Gateway RESTful API。使 API 订阅 Amazon SNS 主题。
 - E. 使消息通道 HTTPS 终端节点订阅 Amazon SNS 主题。
 - F. 编写 AWS Lambda 函数，解决不合规的安全配置。使函数订阅 Amazon SNS 主题。
- 7) 一家公司在运行最新版本 Amazon Linux AMI 的 Amazon EC2 实例上运行应用程序。应用新的安全补丁时，服务器管理员手动移除受影响的运行中实例、对实例打补丁，然后将实例重新投入使用。新的公司安全政策要求在安全补丁发布后的 7 天内应用补丁。安全团队必须确保所有实例都合规。修补操作应该在对用户影响最小的时段内完成。

管理员如何自动执行安全政策合规流程？

- A. 配置 AWS CodeBuild 项目，通过 SSH 下载补丁并应用到所有计算机。使用 Amazon CloudWatch Events 计划的事件，在维护时段中运行 CodeBuild 项目。
- B. 使用 AWS Systems Manager Patch Manager 创建补丁基准。在 EC2 实例上创建脚本，该脚本使用 CLI 从 Patch Manager 提取最新的补丁。创建 cron 作业，计划脚本在维护时段中运行。
- C. 创建应用任意可用安全补丁的脚本。创建 cron 作业，计划脚本在维护时段中运行。在应用程序 AMI 中安装脚本和 cron 作业，并重新部署应用程序。
- D. 在补丁组中列出所有应用程序 EC2 实例。使用 AWS Systems Manager Patch Manager 创建补丁基准。配置维护时段以应用补丁基准。

AWS 认证开发运维工程师 - 专业级
AWS Certified DevOps Engineer - Professional
(DOP-C01) 考试样题

- 8) 操作员正在管理 AWS 上的旧应用程序。该应用程序是运行在单个 Amazon EC2 实例上的整体式 Microsoft Windows 程序。应用程序的源代码不可用，因此无法修改应用程序。应用程序出现内存泄露和故障，实例上的内存利用率超过 90%。操作员在 EC2 实例上配置了统一 Amazon CloudWatch 代理，用来收集内存利用率性能监视器计数。

操作员应采取什么措施来防止应用程序出现故障？（选择两项。）

- A. 创建在内存利用率超过 80% 时发布到 Amazon SNS 主题的 Amazon CloudWatch Events 事件。
 - B. 创建针对 Amazon CloudWatch Logs 中的内存利用率的指标筛选条件。创建针对内存利用率筛选条件的 CloudWatch 警报，该警报在内存利用率超过 80% 时发布到 Amazon SNS 主题。
 - C. 创建针对内存利用率指标的 CloudWatch 警报，该警报在内存利用率超过 80% 时发布到 Amazon SNS 主题。
 - D. 使 Amazon Lambda 函数订阅 Amazon SNS 主题，该函数使用 SNS Run Command 重新启动应用程序。
 - E. 使 EC2 实例订阅 Amazon SNS 主题并运行重新启动应用程序的脚本。
- 9) 一家公司正在将超过 100 个内部应用程序迁移到 AWS。这些应用程序是独立的，但使用相似的公司标准架构。架构的主要不同之处在于：
- 某些应用程序同时具有 Web 层和应用层，而其他应用程序只有 Web 层。
 - 如果有数据库，则为 MySQL、SQL Server 或 PostgreSQL。（该公司计划通过 Amazon RDS 管理所有数据库。）
 - 一些应用程序构建在 LAMP 堆栈上，而另一些构建在 .NET 堆栈上。

开发运维团队希望使每个应用程序团队能够启动基础设施来部署自己的应用程序。与此同时，开发运维团队希望限制各个团队在公司标准之外启动基础设施的能力。

哪种方法使得团队能够以最小权限为其应用程序启动基础设施？

- A. 创建两个 AWS Service Catalog 产品：一个创建两层架构，另一个创建三层架构。将技术堆栈和数据库技术作为参数传入。授予应用程序团队启动产品所需的权限。
 - B. 创建两个 AWS CloudFormation 模板：一个创建两层架构，另一个创建三层架构。将技术堆栈和数据库技术作为参数传入。授予应用程序团队创建 CloudFormation 堆栈所需的权限。
 - C. 创建启动 AWS Elastic Beanstalk Web 服务器环境应用程序的 AWS CloudFormation 模板。将层数、技术堆栈和数据库技术作为参数传入。授予应用程序团队创建 CloudFormation 堆栈所需的权限。
 - D. 创建启动 AWS Elastic Beanstalk Web 服务器环境应用程序的 AWS Service Catalog 产品。将层数、技术堆栈和数据库技术作为参数传入。授予应用程序团队启动产品所需的权限。
- 10) 一家公司针对 Amazon RDS PostgreSQL 多可用区数据库实例设计了跨区域灾难恢复解决方案。该灾难恢复解决方案需要 4 小时的 RPO 和 2 小时的 RTO。

哪个解决方案能够以最经济高效的方式满足这些要求？

AWS 认证开发运维工程师 - 专业级
AWS Certified DevOps Engineer - Professional
(DOP-C01) 考试样题

- A. 创建一个 AWS Lambda 函数，该函数创建 RDS 快照并将其复制到其他区域。创建每 4 个小时触发 Lambda 函数的 Amazon CloudWatch Events 计划事件。创建 RDS 通知事件以发布数据库可用性事件的 Amazon SNS 消息。将 Lambda 函数订阅到 SNS 主题，该函数将快照恢复到灾难恢复区域中的新实例，并更新应用程序的连接字符串。
- B. 创建一个 AWS Lambda 函数，该函数生成 SQL 转储文件并将文件保存到其他区域的 Amazon S3 存储桶中。创建每 4 个小时触发 Lambda 函数的 Amazon CloudWatch Events 计划事件。创建 RDS 通知事件以发布数据库可用性事件的 Amazon SNS 消息。将 Lambda 函数订阅到 SNS 主题，该函数启动新数据库实例、执行 SQL 转储文件并更新应用程序的连接字符串。
- C. 创建一个 AWS Lambda 函数，该函数将最新的自动快照复制到其他区域。创建每 4 个小时触发 Lambda 函数的 Amazon CloudWatch Events 计划事件。创建 RDS 通知事件以发布数据库可用性事件的 Amazon SNS 消息。将 Lambda 函数订阅到 SNS 主题，该函数将快照恢复到灾难恢复区域中的新实例，并更新应用程序的连接字符串。
- D. 为不同区域中的数据库实例配置只读副本。创建 RDS 通知事件以发布数据库可用性事件的 Amazon SNS 消息。创建一个 AWS Lambda 函数，该函数将提升只读副本并更新应用程序的连接字符串。将 Lambda 函数订阅到 SNS 主题。

AWS 认证开发运维工程师 - 专业级
AWS Certified DevOps Engineer - Professional
(DOP-C01) 考试样题

答案

- 1) B - 这是给出选项中响应最快的答案，因为它是确定性的；更改将直接触发事件并且事件将直接触发管道。虽然 A 中所述的定期检查也适用，但并非确定性的，因为它们直到执行下次定期检查时才会启动管道。B 同时还是[建议的解决方案](#)。C 不是 CodeCommit 支持的功能。D 不是启动管道的有效方法。
- 2) A、D - CodeCommit 使用 IAM 策略[授予和拒绝对存储库的访问权限](#)。CloudWatch Events 提供近乎实时的 CodeCommit 事件流，包括[存储库状态更改](#)。CloudWatch Events 规则可以在[事件与某个模式匹配](#)时触发，并将通知发送到 SNS 主题。B 不正确，这是因为 CodeCommit 只支持 IAM 策略，不支持资源策略。C 不正确，这是因为 Lambda 函数检测事件可能需要长达 15 分钟时间。E 不正确，这是因为 CloudTrail 日志记录事件可能需要长达 15 分钟时间。
- 3) C - [S3 默认加密](#)可确保加密静态构件。使用 Deny 语句并将 [NotPrincipal](#) 设置为操作角色时，除了使用该角色的请求之外，会拒绝对存储桶进行的访问。在词干中暗示了操作角色具有权限策略，允许访问存储桶。A 和 B 不正确是因为存储桶策略引用 IAM 组而非角色。A 之所以不正确，还在于 [AWS 建议使用默认加密](#)而不是存储策略来强制实施加密。B 还允许短暂静态存储构件而不加密。D 不正确是因为 AWS KMS 只能加密最多 4 KB 大小的数据。
- 4) B、D、E - 在[蓝/绿部署](#)中具备两个单独的环境，其中蓝色环境包含位于 Auto Scaling 组中的 EC2 实例，运行当前应用程序的生产版本；绿色环境包含 Auto Scaling 组中的另一组 EC2 实例，运行应用程序的新版本。每个 Auto Scaling 组将位于各自的 Application Load Balancer (ALB) 之后，因此您可以在 Route 53 中配置两个别名记录作为终端节点，并使用[加权路由策略](#)从蓝色环境的 ALB 将流量逐渐转移到绿色环境。除非需要对新版本进行架构更改，否则最好将两个环境指向相同的数据库，这样在切换期间数据能够保持一致。A 不正确，这是因为需要两个 ALB 作为终端节点来使用 Route 53 逐步转移流量。C 不正确，这是因为故障转移路由策略只有在运行状况检查检测到出现故障时，才将所有流量发送到单个终端节点，因此无法用于逐步转移流量。F 不正确，这是因为多可用区 RDS 中的第二个实例是热备用实例，不能用于读取或写入。
- 5) B、D、E - 本题的关键在于：在模板中必须有某种方式向 CloudFormation 指示 S3 中的源文件发生了更改，因为 CloudFormation 既不存储源文件的时间戳，也不存储任何类型的校验和。在这些正确答案中，均对模板进行了更改，可能是[版本](#) (B)、[代码位置](#) (D) 或[对象名称](#) (E)。除非对模板进行大量改写，使其成为 SAM 模板 (SAM 是标准 CloudFormation 模板的扩展) 或 serverless.yml 文件，否则 C 和 F 是不可行的。A 会上传新代码，但作为全新的函数，具有新的 ARN 和新的函数名称，需要对模板的其余部分进行更多编辑，同时会断开模板之外依赖于该函数的任何资源。
- 6) B、E、F - 该解决方案分为两部分：发出有关不合规配置的通知，然后配置 SNS 扇出以完成所有提出的要求。B 是发送[有关不合规情况的正确通知](#)的方式。A 和 C 将发送任意配置更改的通知，而不论其合规性状态如何，这会导致收件人需要付出额外的工作来确定每条消息是否重要。使用多个 SNS 终端节点可完成提出的要求。E 使用 SNS [HTTPS 终端节点](#)，在 POST 请求的正文中提供消息。F 使用 SNS [Lambda 终端节点](#)，从 SNS 消息触发 AWS Lambda 函数。D 不会实现任何所需的结果，因为它仅仅将消息发送回 AWS Config 服务。

AWS 认证开发运维工程师 - 专业级
AWS Certified DevOps Engineer - Professional
(DOP-C01) 考试样题

- 7) D - [Patch Manager](#) 将根据您在[补丁基准](#)中定义的已批准补丁列表，在维护时段期间自动应用安全补丁。安全团队可以在 Systems Manager 控制台中查看[补丁合规性](#)，或者使用 CLI 提取概要信息。A 不正确，这是因为 CodeBuild 将您的源代码构建到构件中。它不会将补丁部署到实例。B 不正确，这是因为不需要计划 AWS Systems Manager Agent 来提取补丁。您只需要将修补配置与 [Systems Manager 维护时段](#) 关联起来即可。C 不正确，这是因为它没有安全团队用于验证补丁合规性的方式，并且会在 cron 作业中包括单点故障。
- 8) C、D - 这个问题分为两个部分。第一个部分是，统一 CloudWatch 代理如何发布系统级指标？这些指标作为 [CloudWatch 指标](#) 发布，可以像任何其他指标一样直接用于警报，因此 C 是正确答案。代理将日志文件从 EC2 实例发布到 [CloudWatch Logs](#)，因此 B 不正确。CloudWatch Events 是 CloudWatch 的不同功能，根据系统事件或按计划触发事件，因此 A 不正确。问题的第二个部分是如何采取操作来响应 SNS 消息。EC2 实例无法订阅 SNS 消息，因此 E 不正确。Lambda 函数可以订阅 SNS 消息，因此 D 是正确答案。
- 9) A - AWS Service Catalog 允许管理员发布产品并向 IAM 用户授予[启动产品的权限](#)，而无需向这些用户授予启动底层服务的能力。要启动 CloudFormation 堆栈，用户需要权限来启动堆栈中的所有底层基础设施。虽然有一个功能可以直接通过 IAM 服务角色将权限授予给 CloudFormation，但此处的答案中明确地说明了权限直接授予应用程序团队。Elastic Beanstalk [Web 服务器环境](#) 允许使用单个 Web 层，但不允许同时使用 Web 层和应用层。
- 10) A - 此解决方案通过制作[备用实例的手动快照](#)并将快照复制到不同区域来满足 RPO 要求。RDS 支持可发布到 SNS 主题的[通知事件](#)。Lambda 函数将快照还原到新数据库实例，因此需要在应用程序的连接字符串中更新 DNS 名称。B 是可行的，但 pg_dump 进程将使用主实例上的大量 I/O，而 [RDS 快照是针对辅助实例制作的](#)。此外，大型数据库的 SQL 转储文件会非常大，因此创建新实例然后在转储文件中执行 SQL 命令的过程会超过 2 小时的 RTO。C 不正确，这是因为每天仅创建一次自动快照，因此不满足 RPO 要求。D 是可行的，但由于 RPO 仅为 4 小时，对于这一要求来说，[跨区域读取复制](#)的成本太高。