aws training and certification

AWS 认证开发运维工程师 — 专业级
AWS Certified DevOps Engineer – Professional
（DOP-001）考试样题

1）一家公司正在 AWS CodeCommit 中控制其产品的源代码。该公司使用 AWS CodePipeline 为其产品创建 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，因此需要尽可能提供管道的响应能力。

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。配置管道响应事件而启动。

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，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 开发人员组的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 分钟运行一次的 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。定义指标筛选器来确定存储库事件。创建 CloudWatch 警报，将 Amazon SNS 主题作为目标。

3）公司使用 AWS CodeBuild 来生成其应用程序。公司政策要求对所有生成构件静态加密。对构件的访问限制为有权限承担操作角色的 IAM 用户

如何满足这些要求？

A) 添加生成后命令到 CodeBuild 生成规范，该命令将生成对象推送到 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。对于 `NotPrincipal` 部分引用操作 IAM 组的所有操作，添加 `Deny` 语句。

B) 添加生成后命令到 CodeBuild 生成规范，该命令将生成对象推送到 Amazon S3 存储桶。配置 S3 事件通知以触发 AWS Lambda 函数来获取对象、加密对象，然后将其放回到具有 `encrypted` 标签键和 `true` 标签值的 S3 存储桶。对于 `NotPrincipal` 部分引用操作 IAM 组并且 `Condition` 部分引用 `Encrypted` 的所有操作，添加具有 `Deny` 语句的 S3 存储桶策略。

C) 添加生成后命令到 CodeBuild 生成规范，该命令将生成对象推送到启用了 S3 默认加密的 Amazon S3 存储桶。设置 S3 存储桶策略，其中对于 `NotPrincipal` 部分引用操作 IAM 角色的所有操作，包含一条 `Deny` 语句。

D) 添加生成后命令到 CodeBuild 生成规范，该命令调用 AWS KMS `Encrypt` API，将构件传递到 AWS KMS 以使用指定的客户主密钥（CMK）加密。将加密的构件推送到 Amazon S3 存储桶，然后设置 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 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，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。工程师获取了函数代码的新版本，并希望确保此新版本在堆栈更新之后立即执行。

哪些部署过程可以做到这一点？（选择三项。）

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

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 模板以执行 Lambda 函数版本更新。

D) 更新 CloudFormation 模板中 Lambda 函数的 S3 存储桶属性，以指向不同的存储桶位置。将新代码上传到新 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，以指示 .zip 文件的不同位置和名称。将新代码上传到新 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` 命令以执行对现有 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 规则以检测不合规的安全配置。检测到合规性问题时，公司希望自动修复问题，并且需要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，通过通道发送 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 Amazon API Gateway RESTful API 并具有与 AWS Config 的 AWS 集成。将 API 订阅到 Amazon SNS 主题。
E) 订阅消息通道 HTTPS 终端节点到 Amazon SNS 主题。
F) 编写 AWS Lambda 函数，解决不合规的安全配置。将函数订阅到 Amazon SNS 主题。

7）一家公司正在运行 Amazon Linux AMI 最新版本的 Amazon EC2 实例上运行应用程序。应用新的安全补丁时，服务器管理员手动从服务中删除受影响的实例、打补丁，然后将其放回服务。新的公司安全政策要求在安全补丁发布的 7 天以内应用补丁。安全团队必须确保所有实例都合规。修补操作在对用户影响最小的时段中进行。

管理员如何自动实现安全政策合规？

A) 配置 AWS CodeBuild 项目，通过 SSH 下载并应用补丁到所有计算机。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，使用 CLI 从 Patch Manager 提取最新的补丁。创建 cron 任务以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 任务以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 任务，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。

8）操作员管理 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 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。当实例上的内存利用率超过 90%时应用程序会出现内存泄露和故障。操作员在 EC2 实例上配置了统一 Amazon CloudWatch 代理以收集内存利用率性能监视器计数器。

操作员应采取什么操作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) 将 Amazon Lambda 函数订阅到 Amazon SNS 主题，该函数使用 AWS Systems Manger Run command 重新启动应用程序。

E) 将 EC2 实例订阅到 Amazon SNS 主题并运行重新启动应用程序的脚本。

9）公司正在迁移 100 多款内部应用程序到 AWS。这些应用程序彼此独立，但使用相似的公司标准架构。架构中不同的主要领域在于：

- **一些应用程序同时具有 Web 层和应用层，而一些只有 Web 层。**
- **如果有数据库，则可能是 MySQL、SQL Server 或 PostgreSQL。（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得每个应用程序团队可以启动基础设施来部署自己的应用程序。于此同时，开发运维团队希望限制各个团队启动超出公司标准的基础设施的能力。

哪种方法使得团队能够以最小权限启动其应用程序的基础设施？

A) 创建两个 AWS Service Catalog 产品：一个创建两层架构，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，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）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。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成功满足要求？

A) 创建 AWS Lambda 函数，该函数创建 RDS 快照并将其复制到其他区域。创建 Amazon CloudWatch Events 计划事件来每 4 小时触发一次 Lambda 函数。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 AWS Lambda 函数，该函数生成 SQL 转储文件并将其保存到其他区域的 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 通知事件来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) 创建将最新自动快照复制到其他区域的 AWS Lambda 函数。创建 Amazon CloudWatch Events 计划事件来每 4 小时触发一次 Lambda 函数。创建 RDS 通知事件来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 通知事件来发布数据库可用性事件的 Amazon SNS 消息。创建 AWS Lambda 函数，该函数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。

答案

1) B — 这是给出选项中响应性最好的答案，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，因为它们直到进行下次定期检查时才会启动管道。
B 同样是建议解决方案。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 规则可以通过与某个模式匹配的事件触发，并发送通知到 SNS 主题。B 不正确是因为 CodeCommit 只支持 IAM 策略，不支持资源策略。C 不正确是因为 Lambda 函数检测事件可能需要多达 15 分钟。E 不正确是因为 CloudTrail 日志记录事件可能需要多达 15 分钟。

3) C — S3 默认加密可确保加密静态构件。Deny 语句并将 NotPrincipal 设置为操作角色可拒绝除了使用该角色之外访问存储桶的请求。其主干隐含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 的不正确还在于 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 组将位于自己的 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。除非新版本有必需的架构更改，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保持一致。A 不正确是因为需要两个 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 — 此项目的关键在于在模板中必须有某种方式指示 CloudFormation，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。这些键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 无法使用。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，同时会中断模板之外依赖于函数的任何资源。

6) B、E、F — 解决方案有两个部分：告示全体人有关不合规的配置，然后配置 SNS 扇出以完成所有产生的要求。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，不论其合规性状态，这会导致收件人要做额外的工作来确定每条消息是否重要。使用多个 SNS 终端节点可完成产生的请求。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。

7) D — Patch Manager 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 控制台中查看实例的补丁合规性或者使用 CLI 提取摘要。A 不正确是因为 CodeBuild 将您的源代码生成到构件中。它不部署补丁到实例。B 不正确是因为不需要计划 AWS Systems Manager 代理来提取补丁。您只需要将修补配置与 Systems Manager 维护时段关联起来。C 不正确是因为它没有包括安全团队用于验证补丁合规性的方式，并且在 cron 作业中包括了单点故障。

8) C、D — 这个问题有两个部分。第一个部分是，统一 CloudWatch 代理如何发布系统级别指标？这些指标作为 CloudWatch 指标发布，可以像其他指标一样直接用于警报，因此 C 是正确的。代理从 EC2 实例发布日志文件到 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来触发事件，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 实例无法订阅到 SNS 消息，因此 E 不正确。Lambda 函数可以订阅到 SNS 消息，因此 D 正确。

9) A — AWS Service Catalog 允许管理员发布产品并授予 IAM 用户权限，*以启动产品而无需* 授予这些用户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 服务角色授权权限到 CloudFormation，此处的响应明确说明了权限直接授予了应用程序团队。Elastic Beanstalk Web 服务器环境允许单个 Web 层，但不允许 Web 层和应用层。

10) A — 此解决方案通过获取备用实例的手动快照并将其复制到不同区域来满足 RPO 要求。RDS 支持可以发布到 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 可以发挥作用，但 pg_dump 进程将使用主实例上的大量 I/O，而 RDS 快照是对辅助实例获取。此外，大数据库的 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 命令会超过 2 小时的 RTO。C 不正确是因为每天仅创建一次自动快照，因此不满足 RPO 要求。D 可以发挥作用，但由于 RPO 仅为 4 小时，对于这一要求跨区域读取复制成本太高。