1）一家公司正在将传统应用程序迁移到 Amazon EC2 中。该应用程序使用存储在源代码中的用户名和密码连接到 MySQL 数据库。数据库将迁移到 Amazon RDS for MySQL 数据库实例。在迁移过程中，该公司希望实施安全的方式来存储和自动轮换数据库凭证。

以下哪种方式可以满足这些要求？

A）在 Amazon 系统映像（AMI）的环境变量中存储数据库凭证。通过替换 AMI 来轮换凭证。
B）在 AWS Systems Manager Parameter Store 中存储数据库凭证。配置 Parameter Store 以自动轮换凭证。
C）在 EC2 实例上的环境变量中存储数据库凭证。通过重新启动 EC2 实例来轮换凭证。
D）在 AWS Secrets Manager 中存储数据库凭证。配置 Secrets Manager 以自动轮换凭证。

2）一位开发人员正在设计 Web 应用程序，该应用程序让用户能够发表评论并近乎实时地接收反馈。

哪些架构可以满足这些要求？（选择两项。）

A）创建 AWS AppSync 架构和对应的 API。使用 Amazon DynamoDB 表作为数据存储。
B）在 Amazon API Gateway 中创建 WebSocket API。使用 AWS Lambda 函数作为后端，并使用 Amazon DynamoDB 表作为数据存储。
C）创建由 Amazon RDS 数据库支持的 AWS Elastic Beanstalk 应用程序。配置应用程序以允许长期存在的 TCP/IP 套接字。
D）在 Amazon API Gateway 中创建 GraphQL 终端节点。使用 Amazon DynamoDB 表作为数据存储。
E）在 Amazon CloudFront 上启用 WebSocket。使用 AWS Lambda 函数作为源，并使用 Amazon Aurora 数据库集群作为数据存储。

3）一位开发人员正在向应用程序添加注册和登录功能。该应用程序需要向自定义分析解决方案发出 API 调用，以便记录用户登录事件。

该开发人员应该使用哪些操作的组合来满足这些要求？（选择两项。）

A）使用 Amazon Cognito 提供注册和登录功能。
B）使用 AWS IAM 提供注册和登录功能。
C）配置 AWS Config 规则，以便执行通过身份验证后事件触发的 API 调用。
D）调用 Amazon API Gateway 方法，以便执行通过身份验证后事件触发的 API 调用。
E）执行 AWS Lambda 函数，以便执行通过身份验证后事件触发的 API 调用。

4）一家公司为 AWS 账户中的 REST API 使用 Amazon API Gateway。安全团队希望只允许来自另一个 AWS 账户的 IAM 用户访问这些 API。

安全团队应该使用哪个操作组合来满足这些要求？（选择两项。）

A) 创建 IAM 权限策略并将该策略附加到各个 IAM 用户。将 API 方法授权类型设置为 AWS_IAM。使用签名版本 4 对 API 请求进行签名。
B) 创建 Amazon Cognito 用户池并将各个 IAM 用户添加到池中。将 API 的方法授权类型设置为 COGNITO_USER_POOLS。使用 Amazon Cognito 中的 IAM 凭证进行身份验证，并将 ID 令牌添加到请求标头。
C) 创建 Amazon Cognito 身份池并将各个 IAM 用户添加到池中。将 API 的方法授权类型设置为 COGNITO_USER_POOLS。使用 Amazon Cognito 中的 IAM 凭证进行身份验证，并将访问令牌添加到请求标头。
D) 为 API 创建仅允许各个 IAM 用户访问的资源策略。
E) 为 API 创建仅允许各个 IAM 用户访问的 Amazon Cognito Authorizer。将 API 的方法授权类型设置为 COGNITO_USER_POOLS。

5）一位开发人员正在构建将文本文件转换为 .pdf 文件的应用程序。这些文本文件由单独的应用程序写入源 Amazon S3 存储桶。该开发人员希望在文件进入 Amazon S3 时读取文件，并使用 AWS Lambda 将这些文件转换为 .pdf 文件。该开发人员编写了 IAM 策略，以允许访问 Amazon S3 和 Amazon CloudWatch Logs。

该开发人员应采取什么操作来确保 Lambda 函数具有合适的权限？

A) 使用 AWS IAM 创建 Lambda 执行角色。将 IAM 策略附加到角色。将 Lambda 执行角色分配给 Lambda 函数。
B) 使用 AWS IAM 创建 Lambda 执行用户。将 IAM 策略附加到用户。将 Lambda 执行用户分配给 Lambda 函数。
C) 使用 AWS IAM 创建 Lambda 执行角色。将 IAM 策略附加到角色。将 IAM 角色作为环境变量存储在 Lambda 函数中。
D) 使用 AWS IAM 创建 Lambda 执行用户。将 IAM 策略附加到用户。将 IAM 用户凭证作为环境变量存储在 Lambda 函数中。

6）一家公司在多个地理位置运行 AWS 工作负载。开发人员在 us-west-1 区域中创建了 Amazon Aurora 数据库。该数据库使用客户托管的 AWS KMS 密钥进行加密。现在，开发人员希望在 us-east-1 区域中创建相同的加密数据库。

开发人员应该采取什么方法来完成此任务？

A）在 us-west-1 区域中创建数据库的快照。将快照复制到 us-east-1 区域并指定 us-east-1 区域中的 KMS 密钥。从复制的快照还原数据库。

B）在 us-west-1 区域中创建数据库的未加密快照。将快照复制到 us-east-1 区域。从复制的快照还原数据库，并使用 us-east-1 区域中的 KMS 密钥启用加密。

C）在数据库上禁用加密。在 us-west-1 区域中创建数据库的快照。将快照复制到 us-east-1 区域。从复制的快照还原数据库。

D）在 us-east-1 区域中，选择还原来自 us-west-1 区域的数据库的最新自动备份。使用 us-east-1 区域中的 KMS 密钥启用加密。

7）一位开发人员正在将 Amazon ElastiCache for Memcached 添加到公司的现有记录存储应用程序中，以减少数据库上的负载并提升性能。根据对常见记录处理模式的分析，该开发人员决定使用延迟加载。

哪个伪代码示例可以正确实施延迟加载？

A）
```
record_value = db.query("UPDATE Records SET Details = {1} WHERE ID == {0}", record_key, record_value)
cache.set (record_key, record_value)
```

B）
```
record_value = cache.get(record_key)
if (record_value == NULL)
    record_value = db.query("SELECT Details FROM Records WHERE ID == {0}", record_key)
    cache.set (record_key, record_value)
```

C）
```
record_value = cache.get (record_key)
db.query("UPDATE Records SET Details = {1} WHERE ID == {0}", record_key, record_value)
```

D）
```
record_value = db.query("SELECT Details FROM Records WHERE ID == {0}", record_key)
if (record_value != NULL)
    cache.set (record_key, record_value)
```

8）一位开发人员希望跟踪运行在 Amazon EC2 实例队列上的应用程序的性能。该开发人员希望跨队列查看和跟踪统计信息，例如请求的平均延迟和最大延迟。在平均响应时间超出阈值时，该开发人员希望立即收到通知。

以下哪种解决方案可以满足这些要求？

A）在各个实例上配置 Cron 作业以测量响应时间，并且每分钟更新一次存储在 Amazon S3 存储桶中的日志文件。使用 Amazon S3 事件通知触发 AWS Lambda 函数，用于读取日志文件并将新条目写入到 Amazon Elasticsearch Service (Amazon ES) 集群中。在 Kibana 控制面板中可视化结果。配置 Amazon ES，在响应时间超过阈值时将警报发送到 Amazon SNS 主题。

B）配置应用程序以将响应时间写入系统日志。安装并配置 Amazon Inspector 代理，以便连续读取日志并将响应时间发送到 Amazon EventBridge。在 EventBridge 控制台中查看指标图。配置 EventBridge 自定义规则，以便在平均响应时间指标超过阈值时发送 Amazon SNS 通知。

C）配置应用程序以将响应时间写入日志文件。在实例上安装并配置 Amazon CloudWatch 代理，以便将应用程序日志流式传输到 CloudWatch Logs。对日志中的响应时间创建指标筛选条件。在 CloudWatch 控制台中查看指标图。创建 CloudWatch 警报，在平均响应时间指标超过阈值时发送 Amazon SNS 通知。

D）在实例上安装并配置 AWS Systems Manager 代理，用于监控响应时间并将其作为自定义指标发送到 Amazon CloudWatch。在 Amazon QuickSight 中查看指标图。创建 CloudWatch 警报，在平均响应时间指标超过阈值时发送 Amazon SNS 通知。

9）一位开发人员正在本地测试应用程序，并已将该应用程序部署到 AWS Lambda。为了避免超过程序包大小限制，部署文件中未包含依赖项。在远程测试应用程序时，由于缺少依赖项，该函数不会执行。

下面哪个方法可解决此问题？

A）使用 Lambda 控制台编辑器更新代码并包括缺少的依赖项。

B）使用缺少的依赖项创建额外的 .zip 文件，并将该文件包含在原始 Lambda 部署程序包中。

C）在 Lambda 函数的环境变量中添加对缺少的依赖项的引用。

D）将包含缺少的依赖项的层附加到 Lambda 函数。

10）一位开发人员正在构建使用 Amazon API Gateway 的 Web 应用程序。该开发人员希望为部署和生产（dev 和 prod）工作负载维护不同的环境。API 将由 AWS Lambda 函数支持，有两个别名：一个用于 dev，一个用于 prod。

如何使用最少数量的配置实现此功能？

A）为每个环境创建 REST API，并将 API 与 Lambda 函数的对应 dev 和 prod 别名集成。然后将两个 API 部署到其相应的阶段并使用阶段 URL 进行访问。

B）创建一个 REST API 并将其与 Lambda 函数集成，并使用阶段变量来替换别名。然后将 API 部署到两个不同的阶段 dev 和 prod，在各个阶段中创建阶段变量，并以不同别名作为值。使用不同的阶段 URL 访问 API。

C）创建一个 REST API 并将其与 Lambda 函数的 dev 别名集成，然后将其部署到 dev 环境。为 prod 配置金丝雀版本部署，在 prod 中金丝雀版本将与 Lambda prod 别名集成。

D）创建一个 REST API 并将其与 Lambda 函数的 prod 别名集成，然后将其部署到 prod 环境。为 dev 配置金丝雀版本部署，在 dev 中金丝雀版本将与 Lambda dev 别名集成。

答案

1) D — AWS Secrets Manager 有助于保护访问数据库、应用程序、服务和其他 IT 资源所需的凭证。该服务使用户可以在数据库凭证、API 密钥和其他密钥的整个生命周期内轻松地对其进行轮换、管理和检索。用户和应用程序使用对 Secrets Manager API 的调用来检索密钥，而无需在纯文本中对敏感信息进行硬编码。使用与 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 的内置集成，Secrets Manager 可提供密钥轮换。

2) A，B — AWS AppSync 允许用户创建灵活的 API 来安全地访问、操作和组合来自一个或多个数据源的数据，从而简化了应用程序开发。AWS AppSync 是一项托管服务，使用 GraphQL 让应用程序可以轻松地获取所需的确切数据。AWS AppSync 允许用户在一系列数据源（包括 Amazon DynamoDB）上构建可扩展的应用程序，包括需要实时更新的应用程序。在 Amazon API Gateway 中，用户可以创建 WebSocket API 作为 AWS 服务（例如 AWS Lambda 或 DynamoDB）或 HTTP 终端节点的有状态前端。WebSocket API 根据从客户端应用程序收到的消息内容来调用后端。与接收和响应请求的 REST API 不同，WebSocket API 支持客户端应用程序与后端之间的双向通信。

3) A，E — Amazon Cognito 可轻松快速地将用户注册、登录和访问控制功能添加到 Web 及移动应用程序。用户还可以创建 AWS Lambda 函数来向自定义分析解决方案发出 API 调用，然后使用 Amazon Cognito 身份验证后触发器触发该函数。

4) A，D — 一个资源策略可用于向一个 AWS 账户中的用户授予对另一个 AWS 账户的 API 访问权限，使用的协议为签名版本 4 (SigV4)。

5) A — AWS Lambda 函数的执行角色向该函数授予访问 AWS 服务和资源的权限。用户在创建函数时提供此角色，而 Lambda 在调用函数时代入该角色。

6) A — 如果用户复制加密快照，则还必须加密快照的副本。如果用户跨区域复制加密的快照，由于 KMS 密钥特定于具体区域，所以用户不能为复制操作使用与源快照相同的 AWS KMS 加密密钥。用户必须改为指定在目标区域中有效的 KMS 密钥。

7) B — 延迟加载是延迟到需要某个记录时才加载该记录的概念。延迟加载功能首先检查缓存。如果记录不存在，则延迟加载功能从数据库中检索记录，然后将记录存储在缓存中。

8) C — Amazon CloudWatch 代理可以配置为将日志和指标流式传输到 CloudWatch。指标筛选条件可以从存储在 CloudWatch Logs 中的日志创建。

9) D — 用户可以配置 AWS Lambda 函数，按照层的格式提取额外的代码和内容。层是包含库、自定义运行时或其他依赖项的 .zip 存档。利用层，用户可以在函数中使用库，而不必将库包含在部署程序包中。

10）B — 利用 Amazon API Gateway 中的部署阶段，用户可以管理各个 API 的多个发布阶段，例如 Alpha 测试、Beta 测试和生产。使用可配置的阶段变量，API 部署阶段可以与不同后端终端节点交互。用户可以使用 API Gateway 阶段变量，通过多个版本和别名引用单个 AWS Lambda 函数。