Q1.一家电子商务公司正在改造其IT基础设施并计划使用AWS服务.公司的CIO要求解决方案架构师设计一个简单、 高可用性和松散耦合的订单处理应用程序.该应用程序负责接收和处理订单.然后再将它们存储在Amazon DynamoDB 表中.该应用程序具有零星的流量模式，应该能够在营销活动期间进行扩展，以便以最小的延迟处理订单.以下哪项是满足 要求的最可靠方法？

1. 在Amazon EC2托管的数据库中接收订单并使用EC2实例处理它们.
2. 在Amazon SQS队列中接收订単并触发AWS Lambda函数来处理它们.
3. 使用AWS Step Functions程序接收订单并触发Amazon ECS容器来处理它们.
4. 在Amazon Kinesis Data Streams中接收订单并使用Amazon EC2实例进行处理.

答案:B

解析：

1. 真的很糟糕...
2. Lambda函数更加可靠和可扩展
3. 这不是step函数的用途
4. 需要配置 auto scale.而 kinesis 没冇 item level ack

Q2.解决方案架构师必须为大量混合的Windows和Unux服务器制定修补计划.修补计划必须安全实施，做好审计准备， 并符合公司的业务要求.哪个选项将以最小的努力满足这些要求？

1. 安装并使用操作系统本地补丁服务来管理所有实例的更新频率和发布批准.使用AWS Config验证毎个实例上的操作 系统状态并报告任何补丁合规性问题.
2. 在所有实例上使用AWS Systems Manager来管理补「.在生产环境之外测试补「，然后在获得适当批准的维护窗口 期间进行部署.
3. 使用AWS OpsWorks for Chef Automate运行一组脚本，这些脚本将遍历给定类型的所有实例.发出适当的操作系统 命令以在每个实例上获取和安装更新，包括在维护窗口期间任何需要的重启.

D.将所有应用程序迁移到AWS OpsWorks并使用OpsWorks自动修补支持在初始安装后使操作系统保持最新.使用 AWS Config提供审计和合规性报告.

答案:B

解析：

A.AWS Config无法监控操作系统状态

C.对于OpsWorks,建议的方法是替换旧实例，并在设置期间应用安全更新

<https://docs.aws.amazon.com/opsworks/latest/userguide/workingsecurity-updates.html> D.OpsWork 自动修补仅在安装 时更新实例 [https://docs.aws.amazon.com/opsworks/latest/用户指南/workingsecurity-updates.html](https://docs.aws.amazon.com/opsworks/latest/%e7%94%a8%e6%88%b7%e6%8c%87%e5%8d%97/workingsecurity-updates.html)

Q3.一家公司拥有一个由Amazon CloudFront, Amazon API Gateway和AWS Lambda函数组成的无服务器应用程序. 目前应用程序代码的部署过程是创建新版本号的Lambda函数并运行AWS CLI脚本进行更新.如果新函数版本有错误， 另一个CLI脚本会通过部署该函数的先前工作版本来恢复.该公司希望减少部署Lambda函数提供的新版本应用程序逻 辑的时间，并减少发现错误时进行检测和恢复的时间.

如何做到这一点？

1. 创建和部署嵌套的AWS CloudFormation堆栈，父堆栈由AWS CloudFront分配和API网关组成，子堆栈包含 Lambda函数.对于Lambda的更改，创建一个AWS CloudFormation更改集并部署；如果触发了错误，则将AWS CloudFormation更改集恢复为之前的版本.
2. 使用AWS SAM和内置的AWS CodeDeploy部署新的Lambda版本，逐步将流屋转移到新版本，并使用流量前和流 量后测试功能来验证代码.如果触发了 Amazon CloudWatch警报，則回滚.
3. 将AWS CLI脚本取构为部署新Lambda版本的单个脚本.

部署完成后，将执行脚本测试.如果检测到错误，请恢复到以前的Lambda版本.

1. 创建并部署一个AWSCloudFormation堆栈,其中包含一个引用新Lambda版本的新API网关端点.将CloudFront 源更改为新的API网美终端节点，监控错误，如果检测到错误，则将AWS CloudFront源更改为以前的API网美终端 节点.

答案:B

解析：

1. Could将其用于回滚触发器.但问题是API网关在更新或回滾时也需要更新以指向不同的lambda版本
2. 最佳实践
3. 需要更新api网关指向其他版本
4. 不是自动的.此外，可能无法使用具有相同URL的API网关端点

Q4. -家公司将多个AWS账户使用AWS Organizations和服务控制策略（SCP）.管理员创建了以下SCP并将其附加 到包含AWS账户1111-1111-1111的组织单位（0U）:

{  
''Version'': ''2012.-10-17 '',   
''Statement'':[   
{  
 ''Sid'': ''AlowsAllActions'',

"Effect '':''Allow'',  
''Action'':''\*'',  
"Resource":"\*"  
 },  
 {  
''Sid'': ''DenyCloudTrail'',  
"Effect '':''Deny'',  
''Action'':''cloudtrail:\*''，  
"Resource":"\*"  
 }   
 ]   
}

''版本''：''2012-10-27"  
''陈述''：［  
 {  
 ''概述"："AllowsAIIActions",  
 ''效果''：''允许"，.  
 ''行动''：''\*''  
 ''资源''：''\*''  
 ''概述''：''DenyCloudTrail",  
 ''效果''："拒绝"，  
 ''行动''："云轨迹：\*''  
 ''资源''：''\*''  
 }  
 ]  
}

在帐户1111-1111-1111中工作的开发人员抱怨他们无法创建Amazon S3存储桶. 管理员应该如何解决这个问题？

1. 给SCP添加带有“允许”效果的s3:CreateBucket.
2. 将账号从OU中移除，将SCP直接附加到账号1111-1111-1111.
3. 指示开发人员将Amazon S3权限添加到他们的IAM实体.
4. 从帐户 1111-1111-1111 中删除 SCP.

答案:C

解析：

1. 它将授予其他人创建S3存储桶的权限.B.不符合组织规定，将账户从OU中移除.而且它也不会起作用.C.添加仅 对开发人员的访问权限，不影响其他人，正确的选项.D、提供人改云道，应禁止.
2. 明确拒绝将覆盖任何允许

<https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html> B.仍会停止动作

1. IAM不能覆盖SCP,两者都需要允许该动作，但策略没有拒绝create s3 bucket *m*
2. 会工作，可能不是最好的选择

某处应该有一篇SCP,但B,D看起来根本不正确. <https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html>

Q5.一家金融公司正在当前一代的Linux EC2实例上运行其关錘业务应甬程序.该应用程序包括一个自我管理的MySQL 数据库，用于执行繁重的I/O操作.该应用程序运行良好，可以在一个月内处理适量的流量.但是，由于月末报告，它在每 个月的最后三天放慢速度，尽管该公司在其基础架构中使用Elastic Load Balancer和Auto Scaling来满足不断增长的 需求.以下哪项操作可以让数据库以对性能影响最小的方式处理月末负载？

1. 预热弹性负载均衡器，使用更大的实例类型，将所有Amazon EBS卷更改为GP2卷.
2. 将数据库集群一次性迁移到Amazon RDS.并创建几个额外的只读副本来处理月末的负载.
3. 将Amazon CloudWatch与AWS Lambda结合使用，根据特定的CloudWatch指标更改集群中Amazon EBS卷 的类型、大小或IOPS.
4. 通过在月底之前拍摄快照并在之后恢复，用具有最大可用存储大小和每秒I/O的新PIOPS卷替换所有现有的 Amazon EBS 卷.

答案:B

解析：

A\C\D：不会解决问题，因为瓶颈在数据库±. Amazon ELB能够为我们的客户处理绝大多数用例，而无需“预热”（根据 预期流量配置负载均衡器以具有适当的容量级别）.在某些情况下，例如当预期流量为闪存时，或者在无法配置负载测试 以逐渐增加流量的情况下，我们建议您联系我们对您的负载均衡器进行“预热”.然后，我们将根据您预期的流量配置负载均 衡器以具有适当的容量级别.我们需要知道您的测试的开始和结束日期或预期的闪存流量、预期的每秒请求速率以及您将 测试的典型请求/响应的总大小.

A：不合适，因为预热ELB需要联系AWS,如果预计流量在5分钟内突然增加，建议这样做・

C：不实用.

D：没有增加多少增强.再加上这个问题从来没有谈到快照！

Q6.-家公司正在使用AWS CloudFormation部署其基础设施.该公司担心，如果删除生产CloudFormation堆栈，存储 在Amazon RDS数据库或Amazon EBS卷中的重要数据也可能会被删除.公司如何防止用户以这种方式不小心删除数 据？

1. 修改CloudFormation模板以将DeletionPolicy属性添加到RDS和EBS资源.
2. 配置不允许删除RDS和EBS资源的堆栈策略.
3. 修改IAM策略以拒绝删除标有Maws:cloudformation:stackname"标签的RDS和EBS资源.
4. 使用AWS Config规则防止删除RDS和EBS资源.

答案:A

解析：

使用DeletionPolicy属性，您可以在资源堆栈被删除时保留或（在某些情况下）备份资源.您为要控制的每个资源指定一 个DeletionPolicy属性.如果资源没有DeletionPolicy属性，则AWS CloudFormation默认删除该资源.要在删除堆栈时 保留资源，请为该资源指定Retain.您可以对任何资源使用保留.例如，您可以保留恢套堆栈、Amazon S3存储桶或EC2 实例，以便在删除它们的堆栈后可以继续使用或修改这些资源.

<https://docs.aws.amazon.com/AWSCIoudFormation/latest/UserGuide/aws-attribute-deletionpolicy.htmlA.https://aws.amazon.com/premiumsupport/knowledge-center/delete-cf-stack-retain> -resources/ B.Stack 更新栈时使用 的策略

<https://docs.aws.amazon.com/AWSCIoudFormation/latest/UserGuide/protect-stack-resources.html> C.i^将防止故意删 除

D.Config规则用于监控，而不是预防

Q7. •家公司使用Amazon EC2实例部署网络队列来托管博客站点,EC2实例位于Application Load Balancer （ALB） 后面，并配置在Auto Scaling组中.Web应用程序将所有博客内容存储在Amazon EFS卷上.该公司最近为博主添加了 一个功能，可以在他们的帖子中添加视频，吸引了以前10倍的用户流量.在一天的高峰时段，用户在尝试访问网站或观 看视频时会报告缓冲和超时问题.哪个是最具成本效益和可扩展性的部署，可以解决用户的问题？

1. 重新配置Amazon EFS以启用最大I/O.
2. 更新博客站点以使用实例存储卷进行存储.在启动时将站点内容复制到卷，在关闭时复制到Amazon S3.
3. 配置Amazon CloudFront分配.将分发指向S3存储桶，并将视频从EFS迁移到Amazon S3.
4. 为所有套件内容设置一个Amazon CloudFront分配，并将分配指向ALB.

答案:C

解析：

1. 不会有太大帮助，因为EC2可能是瓶颈
2. 事故发生时数据丢失

D.仍然使用EC2服务

Q8.一家公司在AWS上运行物联网平台.位于不同位置的物联网传感器将数据发送到公司在Application Load Balancer 后面运行的Amazon EC2实例上的Node.jsAPI服务器.数据存储在使用4TB通用SSD卷的Amazon RDS MySQL 数据库实例中.该公司在现场部署的传感器数量随着时冋的推移而増加，预计会大幅増长.API服务器一直超载，RDS指 标显示写入延迟很高.以下哪些步骤将永久解决问题并随着新传感器的配置实现増长，同时保持该平台的成本效益？（选 择两项.）

1. 将MySQL通用SSD存储大小调整为6TB以提高卷的IOPS
2. 重新设计数据库层以使用Amazon Aurora而不是RDS MySQL数据库实例并添加只读副本
3. 利用Amazon Kinesis Data Streams和AWS Lambda摄取和处理原始数据
4. 使用AWS-X-Ray分析和调试应用程序问题并添加更多API服务器以匹配负载
5. 重新设计数据库层以使用Amazon DynamoDB而不是RDS MySQL数据库实例

答案:CE

解析： 答案:CE

解析：

A.调整到6TB会将IOPS性能从12288更改为16000,但16000将是通用ssd （gp2）可以达到的最大IO.因此， 这不会永久解决问题.B.理论上Aurora不应该有IOPS问题，但是它仍然有64TB CA流的最大大小限制非常适合这样 的数据处理

1. Dynamo没有最大数据大小限制，很适合这个

Q9.解决方案架构师需要将本地遗留应用程序迁移到AWS.该应用程序在负载平衡器后面的两台服务器上运行.该应用程 序需要一个与服务器网络适配器的MAC地址关联的许可证文件.软件供应商需要12小时才能发送新的许可证文件.该 应用程序还使用具有静态IP地址的配置文件来访问数据库服务器.不支持主机名.

鉴于这些要求，应该采取哪些步骤组合来为AWS中的应用程序服务器启用高可用性架构？（选择两项）

1. 创建•个ENI池.从供应商处为池请求许可证文件，并将许可证文件存储在Amazon S3中创建引导自动化脚本以下 载许可证文件并将相应的ENI附加到Amazon EC2实例
2. 创建一个ENI池.从供应商处为池请求许可证文件，将许可证文件存储在Amazon EC2实例上从实例创建AMI并 将此AMI用于所有未来的EC2实例
3. 创建引导自动化脚本向供应商请求新的许可证文件收到响应后，将许可证文件应用到Amazon EC2实例
4. 编辑引导自动化脚本以从AWS Systems Manager Parameter Store读取数据库服务器IP地址，并将该值注入本地 配置文件
5. 编辑Amazon EC2实例以在配置文件中包含数据库服务器IP地址并更新创建AMI以用于所有未来的EC2实例

答案:AD

解析：

ENI解决Mac地址限制.

将许可证文件放在Amazon S3存储桶上可减少EC2实例的管理开销，因为您可以根据需要轻松添加/删除更多许可证 密钥.在Parameter Store上拥有数据库IP地址可确保所有EC2实例都有一个中心位置来检索IP地址.这也减少了 从EC2实例内部不断更新任何脚本的需要，即使您将来添加/删除更多数据库也是如此.

Q10.一位解决方案架构师正在为一家公司即将推出的新应用程序设计数据存储和检索架构.该应用程序旨在每分钟从世界 各地的设备中提取数百万条小记录.每条记录的大小都小于4 KB,并且需要存储在可以低延迟检索的持久位置.数据是短 暂的，公司只需要存储数据120天，之后可以删除数据.解决方案架构师计算，在•年的时间里，存储需求大约为10-15 TB.哪种存储策略最具成本效益且符合设计要求？

1. 将应用程序设计为将每条传入记录作为单个.CSV文件存储fr： Amazon S3存储桶中，以允许索引检索.配置生命周 期策略以删除超过120天的数据.
2. 设计应用程序以将每条传入记录存储在针对规模正确配置的Amazon DynamoDB表中.配置DynamoDB生存时间 （TTL）功能以删除超过120天的记录.
3. 设计应用程序以将每条传入记录存储在Amazon RDS MySQL数据库的单个表中.运行每晚的cron作业，该作业执 行査询以删除任何超过120天的记录.
4. 将应用程序设计为在将传入记录写入Amazon S3存储桶之前对其进行批处理.更新对象的元数据以包含批处理中的 记录列表，并使用Amazon S3元数据搜索功能检索数据.配置生命周期策略以在120天后删除数据・

答案:B

解析：

B、MOST性价比是关键

A-由于大小限制，S3中没有小csv的值

B-预留容量可能有意义.但1kb需要1个写入单元.高吞吐量变得极其昂贵. <https://segment.com/blog/the-million-dollar-eng-problem/>

如果没有提供足够的容量（即使不使用也要收费），它甚至会更贵15,360 GBxO.25美元=3,840.00美元（数据存储 成本）每月每分钟百万次写入=每秒16667次=66,668.00 WCU = 6,232.45美元预留容量（仍然不确定这是正确的， 因为它看起来很便宜）C-RDS开始有意义

它可以达到80000 IOPS

15,360 GBx 0.125美元x1个实例=1,920.00美元（EBS存储成本）16,667预置IOPSxO.10美元x1个实例= 1,666.70 美元（EBS IOPS 成本）1,920.00 美元 + 1,666.70 美元=3,586.70 美元

存储定价（每月）：3,586.70美元

D - S3元数据搜索功能不存在

Q11. •家企业公司希望允许其开发人员通过AWS Marketplace购买第三方软件.该公司使用启用了全部功能的AWS Organizations账户结构，并且在每个组织单位（OU）中都有•个供釆购经理使用的共享服务账户.采购团队的政策表明， 开发人员应该能够仅从批准列表中获取第三方软件,并使用AWS Marketplace中的Private Marketplace来实现此要求. 采购团队希望Private Marketplace的管理仅限于名为釆购经理角色的角色，该角色可以由采购经理承担.公司中的其他 IAM用户、组、角色和帐户管理员应被拒绝Private Marketplace管理访问.

设计架构以满足这些要求的最有效方法是什么？

1. 在组织中的所有AWS账户中创建•个名为procurement-manager-role的IAM角色.将PowerUserAccess托管 策略添加到角色.将内联策略应用于每个AWS账户中的所有IAM用户和角色，以拒绝对

AWSPrivateMarketplaceAdminFullAccess 托管策略的权限.

1. 在组织中的所有AWS账户中创建•个名为procurement-manager-role的IAM角色.将AdministratorAccess托 管策略添加到角色.使用AWSPrivateMarketplaceAdminFullAccess托管策略定义权限边界并将其附加到所有开发人员 角色.
2. 在组织中的所有共享服务帐户中创建•个名为procurement-manager-role的IAM角色.将 AWSPrivateMarketplaceAdminFullAccess托管策略添加到角色.创建组织根级SCP以拒绝除名为采购经理角色的角色 之外的所有人管理Private Marketplace的权限.创建另•个组织根级SCP以拒绝向组织中的每个人创建名为 procurement-manager-role 的 IAM 角色的权限.
3. 在开发人员将使用的AWS账户中创建•个名为procurement-manager-role的IAM角色.将 AWSPrivateMarketplaceAdminFullAccess托管策略保加到角色.在Organizations中创建•个SCP.以拒绝除名为 procurement-manager-role的角色之外的所有人管理Private Marketplace的权限.将SCP应用于组织中的所有共享 服务帐户.

答案:C

解析：

on "everyone" in the organization表示OU中的每个人，这样开发人员就不会以此名称创建角色来获得权限访问

Q12.—家公司在本地环境中托管一个三层Web应用程序.由于最近流量激增导致停机和重大财务影响，公司管理层已下 令将该应用程序转移到AWS.该应用程序是用NET编写的，并且依赖于MySQL数据库.解决方案架构师必须设计可扩 展且高度可用的解决方案，以满足200, 000名日常用户的需求

解决方案架构师应该采取哪些步骤来设计合适的解决方案？

1. 使用AWS Elastic Beanstalk创建一个具有Web服务器环境和Amazon RDS MySQL多可用区数据库实例的新应 用程序.该环境应在多个可用区中的Amazon EC2 Auto Scaling组前面启动网络负载风衡番(NLB).使用Amazon Route 53别名记录将流量从公司域路由到NLB.
2. 使用AWS CloudFormation在跨越三个可用区的Amazon EC2 Auto Scaling组前面启动包含应用程序负载均衡器 (ALB)的堆栈.该堆栈应使用Retain删除策略启动Amazon Aurora MySQL数据库集群的多可用区部署.使用Amazon Route 53别名记录将流量从公司域路由到ALB.
3. 使用AWS Elastic Beanstalk创建•个自动扩展的Web服务器环境，该环境跨越两个独立的区域，每个区域都有- 个应用程序负载均衡器(ALB).使用跨区域只读副本创建Amazon Aurora MySQL数据库集群的多azZ部署.使用具有 地理临近度路由策略的Amazon Route 53在两个区域之间路由流量.
4. 使用AWS CloudFormation在跨越三个可用区的Spot实例的Amazon ECS集群前面启动包含应用程序负载均衡 器(ALB)的堆栈.该堆栈应启动-个具有快照删除策略的Amazon RDS MySQL数据库实例.使用Amazon Route 53 别名记录将流量从公司域路由到ALB.

答案:B

解析：

Web应用程序需要ALB.多可用区部署应解决高可用性问题.保留删除策略，不删除带有堆栈的数据库.

1. 是错误的，因为它还提到了跨区域只读副本，因此该解决方案在其中一个区域中以只读方式大多无法使用.

Q13.-家公司正在实施AWS Organizations以限制其开发人员仅使用Amazon EC2、Amazon S3和Amazon

DynamoDB. Developers帐户驻留在专门的组织单位(OU)中.解决方案架构师在开发者账户上实施了以下SCP:

,^VersijC^:7 \*\*2012-10-17", 詩麻姦g：［*带*

y : "AllowEq2H,

\ "Effect": ,

小刀 -ActiQpr^K^GS ：\*•\*,

} \*苞）

"E

｝，

*nsia*' ： "ah泗字亍\*',

MEf fect.r : I哉low-,

"S3：

source" : \*\*\*\*\*

部署此策略时,Developers账户中的IAM用户仍然可以使用政策中未列岀的AWS服务吗？ 解决方案衆构幡应该怎么做才能消除开发人员使用本次调査范围之外的服务的能力.

1. 为每个应该被约束的AWS服务创建一个明确的拒绝声明
2. 从开发者账户的OU中删除FullAWSAccess SCP
3. 修改FullAWSAccess SCP以明确拒绝所有服务
4. 在SCP的末尾使用通配符添加明确的拒绝语句.

答案:B

解析：

[https://docs.aws.amazon.eom/organizations/latest/userguide/orgs\_manage\_policies\_scps\_strategies.html#orgs\_polici](https://docs.aws.amazon.eom/organizations/latest/userguide/orgs_manage_policies_scps_strategies.html%23orgs_polici) es\_denylist

Q14. •家公司正在开发•项新服务，该服务将在静态端口上使用TCP进行访问.解决方案架构师必须确保该服务具有高 可用性，跨可用区具有冗余性，并且可以使用可公开访问的DNS名称my.service.com进行访问.该服务必须使用固定 地址分配，以便其他公司可以将地址添加到他们的允许列表中.假设资源部署在单个区域的多个可用区中，哪种方案可以 满足这些要求？

A,使用每个实例的弹性IP地址创建Amazon EC2实例.创建网络负载平衡器(NLB)并公开静态TCP端口.向NLB 注册EC2实例.创建名为my.service的新名称服务器记录集.com,并将EC2实例的弹性IP地址分配给记录集.将 EC2实例的弹性IP地址提供给其他公司以添加到他们的允许列表中.

1. 为应用程序创建Amazon ECS集群和服务定义.为ECS集群创建和分配公网IP地址.创建网络负载平衡器(NLB) 并公开TCP端口.

创建目标组并将ECS集群名称分配给NLB.fr建•个名为my.service.com的A记录集，并将ECS集群的公网IP分配 给该记录集.将ECS集群的公网IP地址提供给其他公司添加到他们的允许列表中.

1. 为服务创建Amazon EC2实例.为每个可用区创建•个弹性IP地址.

创建网络负载平衡器(NLB)并公开分配的TCP端U.将弹性IP地址分配给每个可用区的NLB.创建目标组并向NLB 注册EC2实例.创建-个名为my.service .com的新A (别名)记录集，并将NLB DNS名称分配给该记录集.

1. 为应用程序创建Amazon ECS集群和服务定义.为集群中的每个主机创建和分配公共IP地址.创建应用程序负载均 術器(ALB)并公开静态TCP端口.创建目标组并将ECS服务定义名称分配给ALB.创建一个新的CNAME记录集并 将公共IP地址关联到记录集.将Amazon EC2实例的弹性IP地址提供给其他公司以添加到他们的允许列表中.

答案:C

解析：

NLB每个AZ有一个弹性IP来处理TCP流量.名为my.service.com的别名记录集

Q15.一家公司使用多个AWS账户.DNS记录存储在账户A中Amazon Route 53的私有托管区域中.公司的应用程序 和数据库在账户B中运行.

解决方案架构师将在新的VPC中部署一个两层应用程序.为了简化配置，Amazon RDS终端节点的db.example.com CNAME记录集是在Amazon Route 53的私有托管区域中创建的.

在部署期间，应用程序无法启动.故障排除显示db.example.com在Amazon EC2实例上不可解析.解决方案架构师确认 记录集己在Route 53中正确创建.

解决方案架构师应该采取哪些步骤组合来解决此问题？(选择两个.)

1. 将数据库部署在新VPC中的单独EC2实例上.在私有托管区域中为实例的私有IP创建记录集.
2. 使用SSH连接到应用层EC2实例.将RDS端点IP地址添加到/etc/resolv.conf文件.
3. 创建授权以将账户A中的私有托管区域与账户B中的新VPC相关联
4. 在账户B中为example.com域创建私有托管区域.在AWS账户之间配置Route 53复制.
5. 将账户B中的新VPC与账户A中的托管区域相关联.删除账户A中的关联授权

答案:CE

解析:

<https://aws.amazon.com/premiumsupport/knowledge-center/private-hosted-zone-different-account/> <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private->

associate-vpcs-different-accou nts.html

Q16. •家公司有•个Web应用程序，允许用户上传短视频.这些视频存储在Amazon EBS卷上，并由自定义识别软件 进行分析以进行分类.该网站包含静态内容，这些内容的流量在某些月份达到峰偵.该架构包括在Auto Scaling组中运行 的Amazon EC2实例，用于Web应用程序和在Auto Scaling组中运行以处理Amazon SQS队列的EC2实例.该公 司希望在可能的情况下使用AWS托管服务重新构建应用程序以减少运营开销，并消除对第三方软件的依赖.

哪个解决方案满足这些要求？

1. 将Amazon ECS容器用于Web应用程序，将Spot实例用于处理SQS队列的Auto Scaling组.将自定义软件替 换为Amazon Rekognition以对视频进行分类.
2. 将上传的视频存储在Amazon EFS中并将文件系统挂载到Web应用程序的EC2实例.使用调用Amazon Rekognition API对视频进行分类的AWS Lambda函数处理SQS队列.
3. 在Amazon S3中托管Web应用程序.将上传的视频存储在Amazons S3中.使用S3事件通知将事件发布到

SQS队列.使用调用Amazon Rekognition API对视频进行分类的AWS lambda函数处理SQS队列.

1. 使用AWS Elastic Beanstalk在Auto Scaling组中为Web应用程序启动EC2实例，并启动工作环境来处理SQS 队列.将自定义软件替换为Amazon Rekognition以对视频进行分类.

答案:C

解析：

Q17.一家公司计划将单体应用程序重构为部署在AWS上的现代应用程序设计.CI/CD管道需要升级以支持具有以下要 求的应用程序的现代设计：

••它应该允许更改毎小时发布几次它应该能够尽快回滚更改.

哪种设计会满足这些要求？

1. 部署包含AMI的CI/CD管道以包含应用程序及其配置.

通过替换Amazon EC2实例来部署应用程序.

1. 指定AWS Elastic Beanstalk在二级环境中暂存作为应用程序CI/CD管道的部署目标.要部署，请交换登台和生产环 境 URLS.
2. 使用AWS Systems Manager为每个部署重新配置基础设施更新Amazon EC2用户数据以从amazon S3中提取 最新的代码工件并使用Amazon Route 53加权路由指向新环境.
3. 使用预构建的AMI作为自动缩放事件的一部分推出应用程序更新.使用新版本的AMI添加实例，并在部署事件期间 逐步淘汰使用具有己配置终止策略的版本的先前AMI版本的所有实例.

答案:B

解析：

Q18.公司用户AWS Organizations有•个名为Production的0U来管理多个账户.所有账户都是Production 0U管 理员的成员，使用组织根目录中的拒绝列表SCP来管理对受限服务的访问.

公司最近收购了一个新的业务部门，并将新部门现有的AWS账户邀请到该组织.一旦加入，新业务部门的管理员发现他 们无法更新现有的AWS Config规则以满足公司的要求政策.

哪个选项将允许管理员进行更改并继续执行当前策略，而无需引入额外的长期维护？

1. 删除组织的限制访问AWS Config的根SCP.根据公司的标准AWS Config规则创建AWS Service Catalog产品， 并将它们部署到整个组织，包括新账户.
2. 为新账户创建•个名为Onboarding的临时0U将SCP应用于Onboarding 0U以允许AWS Config操作.完成 对AWS Config的调整后，将新账户移至生产0U.
3. 将组织的根SCP从拒绝列表SCP转换为允许列表SCP,以仅允许所需的服务.临时将SCP应用到组织的根，允 许仅在新账户中对委托人执行AWS Config操作.
4. 为新账户创建•个名为Onboarding的临时ou将SCP应用于Onboarding 0U以允许AWS Config操作.将组织 的根SCP移至生产0U完成对AWS Config的调整后，将新账户移至生产0U.

答案:D

解析：

Q19.天气服务从eu-west-1区域的AWS上托管的Web应用程序提供高分辨率天气图.天气图经常更新并与静态

HTML内容一起存储在Amazon S3中.Web应用程序以Amazon CloudFront为前端：

该公司最近扩展到为us-east-1地区的用户提供服务，这些新用户报告说查看他们各自的天气图有时会很慢.哪些步骤组 合可以解决us-east-1性能问题？（选择两项）

1. 为 eu-west-1 中的 S3 存储桶配置 AWS Global Accelerator 端点.在 us-east-1 中为 TCP 端口 80 和 443 配置 端点组.
2. 在us-east-1中创建一个新的S3存储桶.配置S3跨区域复制从eu-west-1中的S3存储桶同步.
3. 使用Lambda@Edge修改来自北美的请求以使用us-east-1中的S3 Transfer Acceleration端点.
4. 使用Lambda@Edge修改来自北美的请求以使用us east-1中的S3存储桶.
5. 将us-east-1的AWS Global Accelerator端点配置为CloudFront分配上的源.使用Lambda@Edge修改来自北美 的请求以使用新源.

答案:BD

解析：

Q20.一家总部位于东海岸的北美公司正在部署一个在us-east-1区域的Amazon EC2上运行的新Web应用程序.应用 程序应动态扩展以满足用户需求并保持弹性.此外，应用程序必须在us-west-1区域的主动•被动配置中具有灾难恢复功 能.

在us-east-1区域创建VPC后，解决方案架构师应该采取哪些步骤？

1. 在us-west-1 Region创建VPC使用inter.区域VPC对等连接两个VPC.将跨多个可用区(AZ)的应用程序负载均 衡器(ALB)部署到us-east-1区域中的VPC.跨每个区域的多个AZ部署EC2实例，作为跨越两个VPC并由ALB 提供服务的Auto Scaling组的一部分.
2. 将跨多个可用区(AZ)的应用程序负载均衡器(ALB)部署到us-east-1区域中的VPC.跨多个可用区部署EC2实 例作为ALB服务的Auto Scaling组的一部分.将相同的解决方案部署到us-west-1区域.创建一个启用了故障转移路由 策略和健康检查的Amazon Route 53记录集，以提供跨两个区域的高可用性.
3. 在us-west-1区域创建VPC.使用区域间VPC对等连接两个VPC.部署跨两个VPC的应用程序负载均衡器 (ALB).在ALB服务的每个VPC中，跨多个可用区部署EC2实例作为Auto Scaling组的一部分.创建指向ALB的 Amazon Route 53 记录.
4. 将跨多个可用区(AZ)的应用程序负载均衡器(ALB)部署到us east-1区域中的VPC.跨多个可用区部署EC2实 例作为ALB服务的Auto Scaling组的一部分.将相同的解决方案部署到us-west-1区域.在指向该区域中的ALB的每 个区域中创建单独的Amazon Route 53记录.使用Route 53健康检査来提供跨两个区域的高可用性.

答案:B

解析：

关键字DR的主动-被动故障转移.我们不需要ALB使用对等跨越VPC.

Q21.-家公司基于部署在AWS CloudFormation堆栈中的AWS Lambda构建了 -个应用程序.Web应用程序的最后 一个生产版本引入了一个导致中断持续几分钟的问题.解决方案架构师必须调整部署过程以支持金丝雀发布.

哪种解决方案可以满足这些要求？

1. 为Lambda函数的每个新部署版本创建一个别名.使用带有routing-config参数的AWS CLI update-alias命令来分 配负载.
2. 将应用程序部署到新的CloudFormation堆栈中.使用Amazon Route 53加权路由策略来分配负载.
3. 为每个新部署的Lambda函数创建一个版本.使用带有routing-config参数的AWS CLI update-function- configuration命令来分配负载.
4. 配置 AWS CodeDeploy 并在 Deploymenl 配置中使用 CodeDeployDefault OneAtATime 来分配负载.

答案:A

解析：

Q22.一家AWS合作伙伴公司使用其名为org1的组织在AWS Organizations中构建了一项服务.此服务要求合作伙伴 公司能够访问客户账户中的AWS资源，该账户位于名为org2的单独组织中.公司必须使用API或命令行脚建立对客 户账户的最低权限安全访问.

允许org1访问org2中的资源的最安全的方法是什么？

1. 客户应向合作伙伴公司提供其AWS账户访问密钥以登录并执行所需任务.
2. 客户应创建-个IAM用户并为IAM用户分配所需的权限.然后，客户应向合作伙伴公司提供凭据以登录并执行所需 的任务.
3. 客户应创建IAM角色并为IAM角色分配所需的权限.然后，合作伙伴公司在请求执行所需任务的访问权限时应使用 IAM角色的亚马逊资源名称(ARN).
4. 客户应创建IAM角色并为IAM角色分配所需的权限.然后，在请求访问权限以执行所需任务时，合作伙伴公司应使 用IAM角色的Amazon资源名称(ARN),包括IAM角色信任策略中的外部ID.

答案:D

解析：

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html>

Q23.解决方案架构师需要就如何将其本地数据处理应用程序迁移到AWS云向公司提供建议.目前，用户通过Web门户 上传输入文件.然后，Web服务器将上传的文件存储在NAS上，并通过消息队列向处理服务器发送消息.每个媒体文件 最多可能需要1小时来处理.该公司己确定，等待处理的媒体文件数量在工作时间显着增加，而在工作时间之后文件数量 迅速下降.

最具成本效益的迁移建议是什么？

1. 使用Amazon SQS创建队列.配置现有Web服务器以发布到新队列.

当队列中有消息时，调用AWS Lambda函数从队列中提取请求并处理文件.将处理后的文件存储在Amazon S3存储桶 中.

1. 使用Amazon MQ创建队列.配置现有Web服务器以发布到新队列.

当队列中有消息时，创建-个新的Amazon EC2实例以从队列中拉取请求并处理文件.将处理后的文件存储在Amazon EFS中.任务完成后关闭EC2实例.

1. 使用Amazon MQ创建队列.配置现有Web服务器以发布到新队列.

当队列中有消息时，调用AWS Lambda函数从队列中提取请求并处理文件.将处理后的文件存储在Amazon EFS中.

1. 使用Amazon SQS创建队列.配置现有Web服务器以发布到新队列.

使用EC2Auto Scaling组中的Amazon EC2实例从队列中提取请求并处理文件.根据SQS队列长度扩展EC2实例. 将处理后的文件存储在Amazon S3存储桶中.

答案:D

解析：

Q24.安全工程师确定现有应用程序从Amazon S3中的加密文件检索Amazon RDS for MySQL数据库的凭证对于应用 程序的下一版本，安全工程师希望实施以下应用程序设计更改以提高安全性：

--数据库必须使用存储在安全AWS托管服务中的随机生成的强密码.

■-应用资源必须通过AWS CloudFormation部署.-应用程序必须每90天轮换一次数据库凭据.解决方案架构师将生成一 个CloudFormation模板来部署应用程序.

CloudFormation模板中指定的哪些资源将以最少的操作开销满足安全工程师的要求？

1. 使用AWS Secrets Manager将数据库密码生成为秘密资源创建一个AWS Larrbda函数资源以轮换数据库密码.指 定Secrets Manager Rotationschedule资源以每90天轮换一次数据库密码.
2. 使用AWS Systems Manager Parameter Store将数据库密码生成为SecureString参数类型创建一个AWS Lambda函数资源以轮换数据库密码指定-个Parameter Store Rotationschedule资源以每90天轮换•次数据库密 码.
3. 使用AWS Secrets Manager生成数据库密码作为秘密资源.创建AWS Lambda函数资源以轮换数据库密码.创建 Amazon EventBridge计划规则资源以每90天触发•次Lambda函数密码轮换.
4. 使用 AWS Systems Manager Parameter Store 将数据库密码生成为 SecureString 参数类型.指定 AWS AppSyn 数 据源资源以每90天自动轮换一次数据库密码.

答案:A

解析：

Q25.一家公司正在本地数据中心运行基于Web的两层应用程序.应用层由运行有状态应用程序的单个服务器组成.该应 用程序连接到在单独服务器上运行的PostgreSQL数据库.

该应用程序的用户群预计将显着增长，因此该公司正在将应用程序和数据库迁移到AWS.

该解决方案将使用 Amazon Aurora PostgreSQL> Amazon EC2 Auto Scaling 和 Elastic Load Balancing.u®种解决方案 将提供一致的用户体验，允许应用程序和数据库层扩展？

1. 为Aurora副本启用Aurora Auto Scaling.使用启用最少未完成请求路由算法和粘性会话的网络负载均衡器.
2. 为Aurora写入器启用Aurora Auto Scaling使用启用了循环路由算法和粘性会话的Application Load Balancer.
3. 为Aurora副本启用Aurora Auto Scaling.使用启用了循环路由算法和粘性会话的Application Load Balancer.
4. 为Aurora writer启用Aurora Auto Scaling.使用启用最少未完成请求路由算法和粘性会话的网络负载均衡器.

答案:C

解析:

Q26.一家公司希望为其每个业务部门更改其内部云计费策略.目前，云治理团队与每个业务部门的负责人共享总体云支出 报告.该公司使用AWS Organizations来管理每个业务部门的单独AWS账户.0rganizations中现有的标记标准包括应 用程序、环境和所有者.云治理团队需要一个集中式解决方案，以便每个业务部门都能收到有关其云支出的月度报告.该解 决方案还应针对任何超过设定阈值的云支出发送通知.哪种解决方案是满足这些要求的最具成本效益的方式？

1. 在每个账户中配置AWS预算并配置按应用程序、环境和所有者分组的预算警报.将每个业务部门添加到每个警报的 Amazon SNS主题.在每个账户中使用Cost Explorer为每个业务部门创建月度报告.
2. 在组织的主账户中配置AWS预算并配置按应用程序、环境和所有者分组的预算警报.将每个业务部门添加到每个警报 的Amazon SNS主题.在组织的主账户中使用Cost Explorer为每个业务部门创建月度报告.
3. 在每个账户中配置AWS预算并配置按应用程序、环境和所有者分组的预算警报.将每个业务部门添加到每个警报的 Amazon SNS主题.使用每个账户中的AWS Billing and Cost Management控制面板为每个业务部门创建月度报告.
4. 在组织的主账户中启用AWS成本和使用报告，并配置按应用程序、环境和所有者分组的报告.创建一个AWS Lambda函数来处理AWS成本和使用情况报告、发送预算警报以及将月度报告发送到每个业务部门的电子邮件列表.

答案:B

解析：

Q27. •家公司有•个本也监控解决方案，使用PostgreSQL数据库来持久保存事件.由于大量摄取，数据库无法扩展，并 且经常耗尽存储空间.该公司想要创建-个混合解决方案，并且已经在其网络和AWS之间建立了 VPN连接.该解决方案 应包括以下属性：

-托管AWS服务以最大程度地降低操作复杂性-•种可自动扩展以匹配数据吞吐量且无需持续管理的缓冲区.-- 种可视化工具，用于创建仪表板以近乎实时地观察事件.一支持半结构化JSON数据和动态模式.哪种组件组合将使公司 能够创建满足这些要求的监控解决方案？(选择两个.)

1. 使用Amazon Kinesis Data Firehose缓冲事件.创建一个AWS Lambda函数来处理和转换事件.
2. 创建一个Amazon Kinesis数据流来缓冲事件.创建一个AWS Lambda函数来处理和转换事件.
3. 配置Amazon Aurora PostgreSQL数据库集群以接收事件.使用Amazon QuickSight从数据库中读取并创建近乎实 时的可视化和控制面板.
4. 配置Amazon Elasticsearch Service (Amazon ES)以接收事件.使用与Amazon ES 一起部署的Kibana端点来创 建近乎实时的可视化和仪表板.
5. 配置Amazon Neptune数据库实例以接收事件.使用Amazon QuickSight从数据库中读取并创建近乎实时的可视化 和控制面板

答案:AD

解析：

Q28.一家公司正在使用AWS Organizations管理多个AWS账户.出于安全目的，公司需要创建一个Amazon Simple Notification Service (Amazon SNS)主题，以便在所有组织成员账户中集成第三方警报系统.解决方案架构师使用AWS CloudFormaticn模板创建SNS主题和堆栈集，以自动部署CloudFormation堆栈.己在组织中启用可信访问.解决方案 架构师应该如何在所有AWS账户中部署CloudFormation StackSets?

1. 在组织成员账户中创建堆栈集.使用服务管理的权限.设置部署选项以部署到组织.使用CloudFormation StackSets偏 差检测.
2. 在组织成员账户中创建堆栈.使用自助服务权限.设置部署选项以部署到组织.启用CloudFormation StackSets自动部 署.
3. 在组织主账户中创建堆栈集.使用服务管理的权限.

设置部署选项以部署到组织.启用CloudFormation StackSets自动部署.

1. 在组织主账户中创建堆栈.使用服务管理的权限设置部署选项以部署到组织.启用CloudFormation StackSets偏差检 测.

答案:C

解析：

Q29.一家生命科学公司正在结合使用开源工具来管理数据分析工作流程，并使用在其本地数据中心的服务器上运行的 Docker容器来处理基因组学数据.测序数据生成并存储在本地存储区域网络(SAN)上,然后对数据进行处理.研发团队遇 到了容量问题，并决定在AWS上重新构建他们的基因组学分析平台，以根据工作负载需求进行扩展，并将周转时间从 几周缩短到几天.

公司拥有高速AWS Direct Connect连接.测序仪将为每个基因组生成大约200 GB的数据；而单个作业可能需要几个小 时才能以理想的计算能力处理数据.最终结果将存储在Amazon S3中.公司预计每天有10-15个工作请求.

哪个解决方案满足这些要求？

1. 使用定期安排的AWS Snowball Edge设备将测序数据传输到AWS.当AWS收到Snowball Edge设备并将数据加 载到Amazon S3时，使用S3事件触发AWS Lambda函数来处理数据.
2. 使用AWS Data Pipeline将测序数据传输到Amazon S3.使用S3事件触发Amazon EC2 Auto Scaling组以启动 运行Docker容器的自定义AMI EC2实例来处理数据.
3. 使用AWS DataSync将测序数据传输到Amazon S3.使用S3事件触发启动AWS Step Functions工作流程的 AWS Lambda 函数糸 Docker 镜像存储在 Amazon Elastic Container Registry (Amazon ECR)中并触发 AWS Batch 运行容器并处理排序数据.
4. 使用AWS Storage Gateway文件网关将测序数据传输到Amazon S3.®用S3事件触发AWS Batch作业，该作业 在运行Docker容器的Amazon EC2实例上执行以处理数据.

答案:C

解析：

Q30. AWS客户有一个在本地运行的Web应用程序.Web应用程序从位于防火墙后面的第三方API获取数据.第三方 只接受每个客户端允许列表中的一个公共CIDR块.

客户希望将其Web应用程序迁移到AWS云.该应用程序将托管在VPC中应用程序负载均衡器(ALB)后面的一组 Amazon EC2实例上.ALB位于公共子网中.EC2实例位于私有子网中.NAT网关提供对私有子网的互联网访问. 解决方案架构师应该如何确保Web应用在迁移后可以继续调用第三方API?

1. 将客户拥有的公共IP地址块关联到VPC.为VPC中的公共子网启用公共IP寻址.
2. 在AWS账户中注册一块客户拥有的公共IP地址.从地址块创建弹性IP地址并将它们分配给VPC中的NAT网 关.
3. 从客户拥有的IP地址块中创建弹性IP地址.将静态弹性IP地址分配给ALB.
4. 在AWS账户中注册一块客户拥有的公共IP地址.设置AWS Global Accelerator以使用地址块中的弹性IP地址. 将AL.B设置为加速器端点.

答案:B

解析：

Q31.公司需要构建混合DNS解决方案.该解决方案将为域cloud.example.com使用Amazon Route 53私有托管区 域，以存储VPC中的资源.公司有如下DNS解析需求：

--本地系统应该能够解析并连接到云.example.com.

--所有VPC都应该能够解析cloud.example .com.

本地企业网络和AWS Transit Gateway之间已经存在AWS Direct Connect连接.

公司应该使用哪种架构来满足这些要求，并提供最高性能？

1. 将私有托管区域关联到所有VPC.在共享服务VPC中创建Route 53入站解析器.将所有VPC附加到中转网关，并 在云的本地DNS服务器中创建转发规则.例如.com指向入站解析器.
2. 将私有托管区域美联到所有VPC.在共享服务VPC中部署Amazon EC2条件转发器.将所有VPC附加到中转网 关，并在指向条件转发器的cloud.example.com的本地DNS服务器中创建转发规则.
3. 将私有托管区域关联到共享服务VPC.在共享服务VPC中创建一个Route 53岀站解析器.将所有VPC附加到中 转网关，并在云的本地DNS服务器中创建转发规则.例如.com指向出站解析器.
4. 将私有托管区域关联到共享服务VPC.在共享服务VPC中创建一个Route 53入站解析器.将共享服务VPC附加 到中转网关，并在本地DNS服务器中为云示例.com创建指向入站解析器的转发规则.

答案:A

解析：

1)所有VPC都应该能够解析私有域，因此所有VPC都应该与托管区域相关联，而不仅仅是共享服务VPC 2)资源存 储在VPC中，而不仅仅是共享服务VPC和本地系统可以连接到整个域.因此，A是正确的，而不是D.该问题询问有 关从 onprem 在 AWS VPC 中访问资源的问题.On Prem -> Inbound End point -> Route 53 resolver -> Resources in connected VPCs ”以上发生在共享服务VPC中--

Q32.一家初创公司使用最新的Amazon Linux2 AMI在私有子网中托管一组Amazon EC2实例.公司的工程师严重依赖 SSH访问实例来进行故障排除.公司现有架构包括以下内容：

■-具有私有子网和公有子网的VPC,以及NAT网关■-用于连接本地环境的站点到站点VPN -EC2安全组，可从本地 环境直接通过SSH访问公司需要增加围绕SSH访问的安全控制，并提供对工程师执行的命令的审计.

解决方案架构师应该使用哪种策略？

1. 在EC2实例队列上安装和配置EC2 Instance Connect.删除附加到EC2实例的所有安全组规则，这些规则允许端 口 22上的入站TCP.建议工程师使用EC2 Instance Connect CLI远程访问实例.
2. 更新EC2安全组以仅允许端口 22上的入站TCP到工程师设备的IP地址.在所有EC2实例上安装Amazon CloudWatch代理并将操作系统审计日志发送到CloudWatch Logs.
3. 更新EC2安全组以仅允许端口 22上的入站TCP到工程师设备的IP地址.为EC2安全组资源更改启用AWS Config.启用AWS Firewall Manager并应用自动修复规则更改的安全组策略.
4. 创建一个附加了 AmazonSSMManagedlnstanceCore托管策略的IAM角色.将IAM角色附加到所有EC2实例.删 除所有附加到允许端口 22上的入站TCP的EC2实例的安全组规则.让工程师为其设备安装AWS Systems Manager 会话管理器插件，并使用Systems Manager的启动会话API调用远程访问实例.

答案:D

解析：

Q33.一家公司将本地数据存储在Windows文件服务器上.公司每天产生5 GB的新数据.该公司将其基于Windows的部分工作负载迁移到AWS,并需要数据在云中的文件系统上可用.该公司已经在本地网络 和AWS之间建立了 AWS Direct Connect连接.公司应该使用哪种数据迁移策略？

1. 使用AWS Storage Gateway中的文件网关选项替换现有的Windows文件服务器，并将现有的文件共享指向新的文 件网关
2. 使用AWS DataSync安排每日任务在本地Windows文件服务器和Amazon FSx之间复制数据
3. 使用 AWS Data Pipeline 安排每日任务在本地 Windows 文件服务器和 Amazon Elastic File System (Amazon EFS) 之间复制数据
4. 使用AWS DataSync安排每日任务在本地Windows文件服务器和Amazon Elastic File System (Amazon EFS)之 间复制数据

答案:B

解析：

Q34. •家公司正在AWS云中开发和托管多个项目.这些项目是跨AWS Organizations中同•组织下的多个AWS账户 开发的.公司要求将云基础设施的成本分配给拥有的项目.负责所有AWS账户的团队发现多个Amazon EC2实例缺少 用于成本分配的项目标签解决方案架构师应该采取哪些措施来解决问题并防止它在未来发生？(选择三项)

1. 在每个账户中创建一个AWS Config规则以查找缺少标签的资源
2. 在组织中创建•个SCP,如果缺少Project标签，则对ec2;Runlnstances执行拒绝操作
3. 在组织中使用Amazon Inspector查找麻少标签的资源
4. 在每个账户中创建一个IAM策略，如果缺少项目标签，则对ec2:Runlnstances执行拒绝操作
5. 为组织创建•个AWS Config聚合器，以收集缺少项目标签的EC2实例列表

F.使用AWS Security Hub聚合缺少项目标签的EC2实例列表

答案:ABE

解析：

Q35.一家公司拥有许多AWS账户，并使用AWS Organizations来管理所有这些账户.解决方案架构师必须实施公司可 用于跨多个帐户共享公共网络的解决方案.

公司的基础设施团队有一个专用的基础设施账户，里面有一个VPC.基础架构团队必须使用此帐户来管理网络个人帐户 无法管理自己的网络.

但是，个人账户必须能够在子网内创建AWS资源.解决方案架构师应该执行哪些操作组合来满足这些要求？(选择两项)

1. 在基础设施账户中创建一个中转网关.
2. 从AWS Organizations主账户启用资源共享.
3. 在AWSOrganizations中的组织内的每个AWS账户中创建VPC配置VPC以与基础设施账户中的VPC共享相 同的CIDR范围和子网将每个单独账户中的VPC与基础设施账户中的VPC对等.
4. 在基础设施账户的AWS Resource Access Manager中创建资源共享选择将使用共享网络的特定AWS Organizations 0U选择每个了网以与资源共享关联.
5. 在基础设施账户的AWS Resource Access Manager中创建资源共享选择将使用共享网络的特定AWS Organizations 0U选择每个前缀列表以与资源共享关联.

答案:BD

解析：

Q36.一家大公司正在运行一个流行的Web应用程序.该应用程序在私有子网中的Auto Scaling组中的多个Amazon EC2 Linux实例上运行.

Application Load Balancer以私有子网中Auto Scaling组中的实例为目AWS Systems Manager会话管理器已配 置，AWS Systems Manager代理正在所有EC2实例上运行.

该公司最近发布了新版本的应用程序一些EC2实例现在被标记为不健康并被终止.

因此，应用程序正在以减少的容量运行.解决方案架构师试图通过分析从应用程序收集的Amazon CloudWatch日志来确 定根本原因，但日志是不确定的.解决方案架构师应如何访问EC2实例以解决问题？

1. 暂停 Auto Scaling 组的 HealthCheck 缩放过程.

使用会话管理器登录到标记为不健康的实例

1. 启用EC2实例终止保护.

使用会话管理器登录到标记为不健康的实例.

1. 在Auto Scaling组上将终止策略设置为Oldestlnstance使用会话管理器登录到标记为不健康的实例.
2. 暂停 Auto Scaling 组的 Terminate 进程.

使用会话管理器登录到标记为不健康的实例.

答案:D

解析：

因为它会阻止已经标记为不健康的实例终止.

[https://docs.aws.amazon.eom/autoscaling/ec2/userguide/as-suspend-resume-processes.html#choosing-suspend-resu](https://docs.aws.amazon.eom/autoscaling/ec2/userguide/as-suspend-resume-processes.html%23choosing-suspend-resu) me

Q37. •家公司希望将应用程序从在本地数据中心运行的VMware Infrastructure迁移到Amazon EC2.

解决方案架构师必须在迁移期间保留软件和配置设置.解决方案架构师应该怎么做才能满足这些要求？

1. 配置AWS DataSync代理以开始将数据存储复制到Amazon FSx for Windows File Server.

使用SMB共享来托管VMware数据存储.

使用 VM Import/Export 将 VM 移动到 Amazon EC2.

1. 使用VMware vSphere客户端将应用程序导出为开放可视化格式(OVF)格式的图像.

创建•个Amazon S3存储桶以将图像存储在目标AWS区域中.

为VM Import创建并应用IAM角色.

使用AWS CLI运行EC2导入命令.

1. 为文件服务配置AWS Storage Gateway以导出通用Internet文件系统(CIFS)共享.

创建共享文件夹的备份副本.

登录AWS管理控制台并从备价副本创建AMI.

启动基于AMI的EC2实例.

1. 在AWS Systems Manager中为混合环境创建托管实例激活.

在本地VM上下载并安装Systems Manager代理.

使用Systems Manager将VM注册为托管实例.

使用AWS Backup创建VM的快照并创建AMI.

启动基于AMI的EC2实例.

答案:B

解析:

Q38.一家软件公司在AWS上托管一个应用程序，其资源位于多个AWS账户和区域中.该应用程序在位于us・east-1 区域的应用程序VPC中的一组Amazon EC2实例上运行，其IPv4 CIDR块为10.10.0.0/16.在另一个AWS账户中， 共享服务VPC位于us-east-2区域，其IPv4 CIDR块为10.10.10.0/24.当云工程师使用AWS Cloud Formation尝试 将应用程序VPC与共享服务VPC建立对等关系时.错误消息表示对等失败.

哪些因素可能导致此错误？(选择两项)

1. 两个VPC的IPv4 CIDR范围重叠
2. VPC不在同一个Region
3. 一个或两个帐户都没有访问互联网网关的权限
4. 其中一个 VPC 未通过 AWS Resource Access Manager 共享.
5. peer accepter账户中的IAM角色没有正确的权限.

答案:AE

解析： 云工程师使用"AWS CloudFormation”尝试对等应用程序.

Q39.公司需要为其服务器实施补丁程序.本地服务器和Amazon EC2实例使用各种工具来执行修补.管理需要一个单一 的报告来显示所有服务器和实例的补丁状态.解决方案架构师应该采取哪一组操作来瞒足这些要求？

1. 使用AWS Systems Manager管理本地服务器和EC2实例上的补丁.

使用Systems Manager生成补丁合规性报告.

1. 使用AWS OpsWorks管理本地服务器和EC2实例上的补丁.

使用Amazon QuickSight与OpsWorks的集成来生成补丁合规性报告.

1. 使用 Amazon EventBridge (Amazon CloudWatch Events)规则通过安排 AWS Systems Manager 补丁补救作业来 应用补丁.

使用Amazon Inspector生成补丁合规性报告

1. 使用AWS OpsWorks管理本地服务器和EC2实例上的补丁.

使用AWS X-Ray将补丁状态发布到AWS Systems Manage OpsCenter以生成补丁合规性报告.

答案:A

解析：

Q40. •家公司在Amazon EC2 Linux实例上运行专有的无状态ETL应用程序.该应用程序是Linux二进制文件，无法 修改源代码.该应用程序是单线程的，使用2GB的RAM.并且是高度CPU密集型的.该应用程序计划每4小时运行… 次，最多运行20分钟.解决方案架构师想要修改解决方案的架构.

解决方案架构师应该使用哪种策略？

1. 使用AWS Lambda运行应用程序.

使用Amazon CloudWatch Logs每4小时调用一次Lambda函数.

1. 使用AWS Batch运行应用程序.

使用AWS St即Functions状态机每4小时调用•次AWS Batch作业.

1. 使用AWS Fargate运行应用程序.

使用 Amazon EventBridge (Amazon CloudWatch Events)每 4 小时调用-次 Fargate 任务.

1. 使用Amazon EC2 Spot实例运行应用程序.

使用AWS CodeDeploy每4小时部署和运行•次应用程序.

答案:C

解析：

状态机没有调度器功能，需要通过cloudevent等其他服务调用

1)步骤状态机没有时间表2) Fargate任务适合这项工作，可以由EventBridge调用 <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-ecs-tutorial.html> step 函数可以在由 eventbridge 触发 时运行计划任务，但是当您可以通过eventbridge直接调用它时，为什么还要添加复杂层来运行aws batch.提供的链接

<https://aws.amazon.com/pt/blogs/compute/orchestrating-high-performance-computing-with-aws-step-functions-and-aw> s-batch/仅对HPC有意义，这是需要运行的单个实例

A&D没有意义.至于B —错误的原因有两个.首先，这只是一项工作 .....您不会使用StepFunctions添加工作流程.其 次，无法调度StepFunctions.即使您想在这种情况下使用它，您至少也需要使用CloudWatch Events来触发该过程.C 解决了一切，是唯一可行的选择.

Q41.一家公司有50个AWS账户，它们是AWS Organizations中一个组织的成员.每个账户包含多个VPC.该公司希 望使用AWS Transit Gateway在每个成员账户中的VPC之间建立连接.每次创建新成员账户时，公司都希望自动执行 创建新VPC和中转网关附件的过程.哪些步骤组合可以满足这些要求？(选择两个

1. 从主账户中，使用AWS Resource Access Manager与成员账户共享中转网关.
2. 从主账户，使用AWS Organizations SCP与成员账户共享中转网关.
3. 从主账户启动AWS CloudFormation堆栈集，自动在成员账户中创建新的VPC和VPC transit gateway附件. 使用中转网关ID将附件与主账户中的中转网关相关联.
4. 从主账户启动AWS CloudFormation堆栈集，自动在成员账户中创建新的VPC和对等中转网关附件. 使用中转网关服务相关角色与主账户中的中转网关共享附件.
5. 从主账户，使用AWS Service Catalog与成员账户共享中转网关.

答案:AC

解析：

C正确，没有named peering transit gateway attachment.不需要共享.在会员账户中创建后需要接受附件请求peering transit gateway 是 transit gateway 華U transit gateway 的连接，D 错

Q42.一家金融公司在Amazon S3中托管一个数据湖.公司每晚通过SFTP从几个第三方接收财务数据记录.该公司在 VPC的公共子网中的Amazon EC2实例上运行自己的SFTP服务器.文件上传后，通过在同一实例上运行的cron作 业将它们移动到数据湖.

通过使用Amazon Route 53.可以在DNS sftp.example.com上访问SFTP服务器.解决方案架构师应该如何提高

SFTP解决方案的可靠性和可扩展性？

1. 将EC2实例移动到一个Auto Scaling组中.

将EC2实例放在应用程序负裁均衡器(ALB)后面.

更新 Route 53 中的 DNS 记录 sftp.example.com 以指向 ALB.

1. 将 SFTP 服务器迁移到 AWS Transfer for SFTP.

更新Route 53中的DNS记录sftp.example.com以指向服务器端点主机名.

1. 将SFTP服务器迁移到AWS Storage Gateway中的文件网美.

更新Route 53中的DNS记录sftp.example.com以指向文件网关终端节点.

1. 将EC2实例放在网络负载平衡器(NLB)后面.

更新 Route 53 中的 DNS 记录 sftp.example.com 以指向 NLB.

答案：B

Q43.一家公司计划在AWS上托管一个Web应用程序，并希望在一组Amazon EC2实例之间对流量进行负载平衡. 其中一项安全要求是在客户端和Web服务器之间的传输中启用端到端加密.

哪种解决方案可以满足此要求？

1. 将EC2实例放在应用程序负载均衡器(ALB)后面.

使用AWS Certificate Manager (ACM)预置SSL证书，并将SSL证书与ALB相关联.

导出SSL证书并将其安装在每个EC2实例上.配置ALB以侦听端口 443并将流量转发到实例上的端口 443.

1. 将EC2实例与目标组相关联.

使用 AWS Certificate Manager (ACM)预置 SSL 证书.

创建Amazon CloudFront分配并将其配置为使用SSL证书.

将CloudFront设置为使用目标组作为源服务器.

1. 将EC2实例放在应用程序负载均衡器(ALB)后面.

使用AWS Certificate Manager (ACM)预置SSL证书，并将SSL证书与ALB相关联.

提供第三方SSL证书并将其安装在每个EC2实例上.

配置ALB以侦听端口 443并将流量转发到实例上的端口 443.

1. 将EC2实例放在网络负载平衡器(NLB)后面.

提供第三方SSL证书并将其安装在NLB和每个EC2实例上.

配置NLB以侦听端口 443并将流量转发到实例上的端口 443.

答案:C

解析：

Q44.一家公司在一个AWS账户中运行多个工作负载.一项新的公司政策过时了，工程师只能预置批准的资源，并且工程 师必须使用AWS CloudFormation预置这些资源.解决方案架构师需要创建•个解决方案，以对工程师用于访问的IAM 角色实施新限制.

解决方案架构师应该如何创建解决方案？

1. 将包含已批准资源的AWS CloudFormation模板上传到Amazon S3存储桶.

更新工程师IAM角色的IAM策略以仅允许访问Amazon S3和AWS CloudFormation.

使用AWS CloudFormation模板预置资源.

1. 为工程师的IAM角色更新IAM策略，使其具有仅允许配置已批准资源和AWS CloudFormation的权限.

使用AWS CloudFormation模板创建具有批准资源的堆栈.

1. 使用仅允许AWS CloudFormation操作的权限更新工程师IAM角色的IAM策略.

创建•个新的IAM策略，有权配置己批准的资源，并将该策略分配给-个新的IAM服务角色.

在堆栈创建期间将IAM服务角色用于AWS CloudFormation.

1. 在AWS CloudFormation堆栈中配置资源.

更新工程师IAM角色的IAM策略以仅允许访问他们自己的AWS CloudFormation堆栈.

答案:C

解析：

Q45.一家在全球设有办事处的公司拥有到单个AWS区域的单个1 GbpsAWS Direct Connect连接.公司的本地网络使 用该连接与公司在AWS云中的资源进行通信.该连接具有连接到单个VPC的单个专用虚拟接口.

解决方案架构师必须实施在同一区域中添加冗余Direct Connect连接的解决方案.该解决方案还必须在公司扩展到其他 区域时通过同一对Direct Connect连接提供与其他区域的连接.

哪个解决方案满足这些要求？

1. 提供 个Direct Connect网关.从现有连接中删除现有私有虚拟接口.创建第二个Direct Connect连接.在每个连接上 创建•个新的私有虚拟接口，并将两个私有虚拟接口连接到Direct Connect网关.将Direct Connect网关连接到单个 VPC.
2. 保留现有的私有虚拟接口.创建第二个Direct Connect连接.在新连接上创建一个新的私有虚拟接口，并将新的私有虚 拟接口连接到单个VPC.  
   C. 保留现有的私有虚拟接口.创建第二个Direct Connect连接.在新连接上创建•个新的公共虚拟接口，并将新的公共虚 拟接口连接到单个VPC.  
   D. 提供中转网关从现有连接中删除现有的私有虚拟接口.

创建第二个Direct Connect连接在每个连接上创建-个新的私有虚拟接口，并将两个私有虚拟接口连接到中转网关.将 中转网关与单个VPC相关联

答案:A

解析：

Direct Connect网关是全球可用的资源.您可以在任何区域创建Direct Connect网关并从所有其他区域访问它.以下描述 了您可以使用专线网关的场景.

httpsV/docs.aws.amazon.com^irectconnect/latest/UserGuide/direct-connect-gateways-intro.html

该方案忽略了您在所有选项中都需要一个vgw （虚拟专用网关）的事实.所以我假设可以安全地假设它存在并且未被提及

Q46.某公司在AWS Organizations中有一个组织，该组织拥有大量AWS账户.其中一个AWS账户被指定为中转账户， 并具有与所有其他AWS账户共享的中转网关AWS站点到站点VPN连接在公司的所有全球办事处和中转账户之间配 置.该公司在其所有账户上启用了 AWS Config.公司的网络团队需要集中管理属于全球办事处的内部IP地址范围列表， 开发人员将参考此列表以安全地访问其应用程序.哪种解决方案能够以最少的运营开销满足这些要求？

1. 创建•个托管在Amazon S3中并列出所有内部IP地址范围的JSON文件在更新JSON文件时可以调用的每个 账户中配置•个 Amazon Simple Notification Service （Amazon SNS）主题订阅 AWS SNS 主题的 Lambda 函数使用 更新的IP地址范围更新所有相关的安全组规则
2. 创建一个包含所有内部IP地址范围的新AWS Config托管规则.使用规则检查每个帐户中的安全组以确保符合IP 地址范围列表配置规则以自动修复检测到的任何不合规安全组.
3. 在中转账户中，创建一个包含所有内部IP地址范围的VPC前缀列表使用AWS Resource Access Manager与所有 其他账户共享前缀列表.使用共享前缀列表在其他账户中配置安全组规则.
4. 在中转账户中，创建一个包含所有内部IP地址范围的安全组通过使用B<transit-account-id>啲嵌套安全组引用，将其 他账户中的安全组配置为引用中转账户的安全组/sg-1a2b3c4d"

答案:C

Q47 -家公司正在使用多个AWS账户，并且有多个DevOps团队在这些账户中运行生产和非生产工作负载.该公司希 望集中限制对DevOps团队不使用的某些AWS服务的访问.该公司决定使用AWS Organizations并成功邀请所有 AWS账户加入该组织.他们希望允许访问当前正在使用的服务并拒绝一些特定服务.他们还希望将多个帐户作为一个单元 一起管理.

解决方案架构师应该采取哪些步骤组合来满足这些要求？（选择三项）

1. 使用拒绝列表策略.
2. 查看AWS IAM中的访问顾问以确定最近使用的服务.
3. 査看AWS Trusted Advisor报告以确定最近使用的服务.
4. 删除默认的 FullAWSAccess SCP.
5. 定义组织单位（0U）并将成员账户放置在OU中.
6. 删除默认的 DenyAWSAccess SCP.

答案:BDE

解析：

Q48. •家公司使用应用程序负载均衡器（ALB）和托管在Amazon ECS集群中的Docker应用程序来托管社区论坛站 点.站点数据存储在Amazon RDS for MySQL中，容器映像存储在ECR中.公司需要为其客户提供RTO不超过24小 时、RPO不超过8小时的灾难恢复SIA.以下哪种解决方案是满足要求的最具成本效益的方法？

A.使用AWS CloudFormation在两个区域部署相同的ALB、EC2、ECS和RDS资源.

每8小时安排•次RDS快照.使用RDS多区域复制来更新次要区域的数据库副本.如果发生故障，从最新的快照恢复， 并使用Amazon Route 53 DNS故障转移策略自动将客户重定向到次要区域中的ALB.

1. 将Docker镜像分别存储在两个区域的ECR中.每8小时安排•次RDS快照，并将快照复制到次要区域.发生故障时， 使用AWS CloudFormation在次区域部署ALB、EC2、ECS和RDS资源，从最新的快照恢复，更新DNS记录指向次区 域的ALB.
2. 使用AWS CloudFormation在次要区域部署相同的ALB、EC2、ECS和RDS资源.安排每小时RDS MySQL备 份到Amazon S3,并使用跨区域复制将数据复制到次要区域中的存储桶.出现故障时，将最新的Docker镜像导入到 secondary region的Amazon ECR.部署到EC2实例，恢复最新的MySQL备份，更新DNS i己录指向secondary region 的ALB
3. 在AWS Auto Scaling组中使用ALB和用于Docker的最小资源EC2部署在次要区域中部署轻型试点环境，并使 用扩展策略来増加实例大小和节点数量创建RDS的跨区域只读副本数据.万一发生故障.

将副本提升为主，并更新DNS记录以指向第二个区域中的ALB.

答案:B

解析:

Q49.一家公司希望将其数据分析环境从本地迁移到AWS.该环境由两个简单的Nodejs应用程序组成.其中一个应用程 序收集传感器数据并将其加载到MySQL数据库中.另一个应用程序将数据聚合到报告中.当聚合作业运行时，一些加载作 业无法正常运行.

公司必须解决数据加载问题.公司还需要在不中断或更改公司客户的情况下进行迁移.

解决方案架构师应该怎么做才能满足这些要求？

1. 将Amazon Aurora MySQL数据库设置为本地数据库的复制目标.

为Aurora MySQL数据库创建一个Aurora副本，并移动聚合作业以针对Aurora副本运行将收集端点设置为网络负载 均衡器(NLB)后面的AWS Lambda函数.

并使用Amazon RDS Proxy写入Aurora MySQL数据库.同步数据库后，禁用复制作业并重新启动Aurora副本作为主 实例.将收集器DNS记录指向NLB.

1. 设置 Amazon Aurora MySQL 数据库.使用 AWS Database Migration Service (AWS DMS)执行从本地数据库到 Aurora的连续数据复制.移気聚合作业以针对Aurora MySQL数据库运行.将Application Load Balancer (ALB)后面的 收集终端节点设置为Auto Scaling组中的Amazon EC2实例.同步数据库后，将收集器DNS记录指向ALB.从本地切 换到AWS后禁用AWS DMS同步任务.
2. 设置 Amazon Aurora MySQL 数据库 使用 AWS Database Migration Service (AWS DMS)执行从本地数据库到 Aurora的连续数据复制为Aurora MySQL数据库创建一个Aurora副本，并移动聚合作业话针对Aurora副本将收集 端点设置为应用程序负载均衡器(ALB)后面的AWS Lambda函数，并使用Amazon RDS代理写入Aurora MySQL 数据库.同步数据库后，将收集器DNS记录指向ALB.从本地切换到AWS后禁用AWS DMS同步任务.
3. 设置Amazon Aurora MySQL数据库.为Aurora MySQL数据库创建一个Aurora副本，并移动聚合作业以针对 Aurora副本运行 将收集端点设置为Amazon Kinesis数据流.使用Amazon Kinesis Data Firehose将数据复制到 Aurora MySQL数据库.同步数据库后，禁用复制作业并重新启动Aurora副本作为主实例.将收集器DNS记录指向 Kinesis致据流

答案:C

解析：

Q50. •家公司正在Application Load Balancer后面的Auto Scaling组中的多个Amazon EC2实例上运行应用程序.应 用程序的负载全天都在变化，并且EC2实例会定期扩展和扩展.来自EC2实例的日志文件每15分钟被复制到中央 Amazon S3存储桶中.安全团队发现某些己终止的EC2实例中缺少日志文件.

哪•组操作将确保将日志文件从终止的EC2实例复制到中央S3存储桶？

A.创建•个脚本来将日志文件复制到Amazon S3,并将该脚本存储在EC2实例上的-个文件中.创建Auto Scaling生 命周期挂钩和Amazon EventBridge (Amazon CloudWatch Events)规则以检测来自Auto Scaling组的生命周期事件.

在 autoscaling:Ec2 INSTANCE TERMINATING 转换上调用 AWS Lambda 函数以将 ABANDON 发送到 Auto Scaling 组以防止终止，运行脚本以复制日志文件，并使用AWS SDK终止实例.

1. 使用脚本创建AWS Systems Manager文档以将日志文件复制到Amazon S3.创建Auto Scaling生命周期挂钩和 Amazon EventBridge (Amazon CloudWatch Events)规则以检测来自 Auto Scaling 组的生命周期事件.在 autoscaling:EC2INSTANCE TERMINATING 转换上调用 AWS Lambda 函数以调用 AWS Systems Manager API SendCommand操作来运行文档以复制日志文件并将CONTINUE发送到Auto Scaling组以终止实例.
2. 将日志传送速率更改为每5分钟-次.创建脚本以将日志文件复制到Amazon S3,并将脚本添加到EC2实例用户数 据创建 Amazon EventBridge (Amazon CloudWatch Events)规则以检测 EC2 实例终止.从 EventBridge (CloudWatch Events)规则调用AWS Lambda函数，该规则使用AWS CLI运行用户数据脚本以复制日志文件并终止 实例.
3. 使用脚本创建AWS Systems Manager文档以将日志文件复制到Amazon S3创建一个Auto Scaling生命周期挂 钩，用于将消息发布到 Amazon Simple Notification Service (Amazon SNS)主题.从 SNS 通知中，调用 AS Systems Manager API SendCommand操作以运行文档以复制日志文件并将ABANDON发送到Auto Scaling组以终止实例.

答案:B

解析：

Q51.一家公司正在AWS上运行数据密集型应用程序.该应用程序在数百个Amazon EC2实例的集群上运行.一个共享 文件系统也在多个存储200TB数据的EC2实例上运行.该应用程序读取和修改共享文件系统上的数据并生成报告.该 作业每月运行一次，从共享文件系统读取文件子集，大约需要72小时才能完成.计算实例在Auto Scaling组中扩展，但 托管共享文件系统的实例持续运行.计算和存储实例都在同一个AWS区域中.解决方案架构师需要通过普换共享文件系 统实例来降低成本.文件系统必须在72小时运行期间提供对所需数据的高性能访问.哪种解决方案能够在满足这些要求 的同时最大程度地降低总体成本？

1. 将数据从现有共享文件系统迁移到使用S3智能分层存储类的Amazon S3存储桶.在每个月运行该作业之前，使用 Amazon FSxfor Lustre通过延迟加载使用来自Amazon S3的数据创建一个新的文件系统.在作业期冋使用新文件系统 作为共享存储.作业完成后删除文件系统.
2. 将数据从现有共享文件系统迁移到启用了多重附加功能的大型Amazon Elastic Block Store (Amazon EBS)卷，使用 Auto Scaling组启动模板中的用户数据脚本将EBS卷附加到每个实例.在作业期间使用EBS卷作为共享存储.作业完 成后分离EBS卷.
3. 将数据从现有的共享文件系统迁移到使用S3标准存储类的Amazon S3存储桶在每个月运行作业之前，使用

Amazon FSxfor Lustre通过孵化加载使用来自Amazon S3的数据创建一个新的文件系统在作业期间使用新文件系统 作为共享存储.作业完成后删除文件系统

D.将数据从现有的共享文件系统迁移到Amazon S3存储桶在每月运行作业之前，使用AWS Storage Gateway创建 一个文件网关，其中包含来自Amazon S3的数据使用文件网关作为作业的共享存储.作业完成后删除文件网关.

答案:A

解析：

Q52. •家公司有•个本地网站应用程序，可以为潜在的租户和买家提供房地产信息.该网站使用Java后端和NoSQL MongoDB数据库来存储订阅者数据.公司需要将整个应用程序迁移到具有类似结构的AWS.必须部署应用程序以实现高 可用性，并且公司不能对应用程序进行更改.

哪种解决方案可以满足这些要求？

1. 使用Amazon Aurora数据库集群作为订阅者数据的数据库在跨多个可用区的Auto Scaling组中为Java后端应用 程序部署Amazon EC2实例.
2. 使用Amazon EC2实例上的MongoDB作为订阅者数据的数据库在Java后端应用程序的单个可用区中的Auto Scaling组中部署EC2实例
3. 在多个可用区中使用适当大小的实例配置Amazon DocumentDB (与MongoDB兼容)作为订阅者数据的数据库.跨 Java后端应用程序的多个可用区在Auto Scaling组中部署Amazon EC2实例.
4. 在多个可用区中以按需容量模式配置Amazon DocumentDB (兼容MongoDB)作为订阅者数据的数据库在跨多个 可用区的Auto Scaling组中为Java后端应用程序部署Amazon EC2实例.

答案:D

Q53. •个团队为整个公司收集和发送行为数据.该公司运行具有公共子网、私有子网和互联网网关的多AZVPC环境.每 个公共子网还包含•个NAT网关.公司的大部分应用程序都读取和写入Amazon Kinesis Data Streams. 大多数工作负载在私有子网中运行.

解决方案架构师必须审查基础架构.解决方案架构师需要降低成本并维护应用程序的功能.解决方案架构师使用Cost Explorer并注意到EC2-Other类别中的成本•直很高.进涉审查表明，NatGateway-Bytes收费正在增加EC2-Other 类别的成本.

解决方案架构师应该怎么做才能满足这些要求？

1. 启用VPC流日志.使用Amazon Athena分析日志中可以删除的流量确保安全组阻止导致高成本的流量.
2. 将Kinesis Data Streams的接口 VPC终端节点添加到VPC确保应用程序具有正确的IAM权限以使用接口 VPC 终端节点.
3. 启用VPC流日志和Amazon Detective.§看与Kinesis Data Streams无关的流量的检测结果.配置安全组以阻止该 流量.
4. 将Kinesis Data Streams的接口 VPC端点添加到VPC确保VPC端点策略允许来自应用程序的流量.

答案:D

解析：

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html>

Q54. •家公司正在为•款流行的在线游戏制作续集.在发布后的第•周内将有来自世界各地的大量用户玩游戏.目前，该游 戏由部署在单个AWS区域中的以下组件组成：

-存储游戏资产的Amazon S3存储桶.

~存储玩家分数的Amazon DynamoDB表.

解决方案架构师需要设计-个多区域解决方案，以减少延迟、提高可蕭性并且需要最少的实施工作. 解决方案架构师应该怎么做才能满足这些要求？

1. 创建一个Amazon CloudFront分配以提供来自S3存储桶的资产配置S3跨区域复制. 在新区域中创建新的DynamoDB表.使用新表作为DynamoDB全局表的副本目标.
2. 创建一个Amazon CloudFront分配以提供来自S3存储桶的资产配置S3同区域复制.

在新区域中创建新的DynamoDB表 通过使用AWS Database Migration Service （AWS DMS）和变更数据捕获（CDC） 在DynamoDB表之间配置异步复制.

1. 在新的 Region 中再创建一个 S3 bucket.并在 bucket 之间配置 S3 Cross-Region Replication.G'J建一个 Amazon CloudFront分配并配置源故障转移，其中两个源访问每个区域中的S3存储桶.

通过启用Amazon DynamoDB Streams配置DynamoDB全局表，并在新区域中添加副本表.

1. 在同•个 Region 中创建另•个 S3 bucket.弁在 bucket 之间配置 S3 Same-Region Replication.fi'J建•个 Amazon CloudFront分配并配旦源故坍转移，其中两个源访问S3存储桶.在新区域中创建新的DynamoDB表使用新表作为 DynamoDB全局表的副本目标.

答案:C

解析：

Q55.一家公司在AWS Organizations中为其每个工程团队创建了一个0U.每个0U拥有多个AWS账户.该组织拥有 数百个AWS账户.解决方案架构师必须设计一个解决方案，以便每个0U都可以查看其AWS账户的使用成本明细. 哪个解决方案满足这些要求？

1. 使用AWS Resource Access Manager为每个0U创建AWS成本和使用报告（CUR）允许每个团队通过Amazon QuickSight控制面板可视化CUR.
2. 从AWS Organizations主账户创建AWS成本和使用报告（CUR）.

允许每个团队通过Amazon QuickSight控制面板可视化CUR

1. 在每个AWS Organizations成员账户中创建AWS成本和使用报告（CUR）允许每个团队通过Amazon QuickSight 控制面板可视化CUR
2. 使用AWS Systems Manager创建AWS成本和使用情况报告（CUR）.允许每个团队通过Systems Manager OpsCenter仪表板可视化CUR.

答案:B

解析:

B是结束所有OU的所有账单的唯一有效选项.D-不可能您如何使用OpsCenter可视化CUR? A-RAM无法创 建CUR

C-组织效率不髙且不可能，因为它为所有帐户创建一个CURAWS Certified Solutions Architect Professional是一项顶 级AWS认证.非技术人员很难把每道题看几个小时，耗费大量的时间和精力，从而影响自己的工作.如果您不是技术人员 对于考试捷径需求联系微信客服：ANYPASS.我们会帮您轻松轻松通过，当然如果技术人员有需求也可以联系，祝您工 作顺利每次考试都会通过！！

Q56.公司的工厂和自动化应用程序在单个VPC中运行.超过20个应用程序在Amazon EC2> Amazon Elastic Container Service (Amazon ECS)和 Amazon RDS 的组合上运行.

该公司的软件工程师分布在三个团队中.三个团队之•拥有每个应用程序，每个团队负责其所有应用程序的成本和性能团 队资源具有代表其应用程序和团队的标签.

团队使用IAM访问权限进行日常活动

公司需要确定毎月AWS账单上的哪些成本可归因于每个应用程序或团队.公司还必须能够创建报告来比较过去12个 月的成本并帮助预测未来12个月的成本.解决方案架构师必须推荐提供这些成本报告的AWS Billing and Cost Management解决方案.哪种行动组合将满足这些要求？(选择三项)

1. 激活代表应用程序和团队的用户定义的成本分配标签.
2. 激活代表应用程序和团队的AWS生成的成本分配标签
3. 为Billing and Cost Management中的每个应用程序创建一个成本类别
4. 激活 IAM 对 Billing and Cost Management 的访问
5. 创建成本预算.
6. 启用 Cost Explorer

答案:ADF

解析:

Q57. •家公司想要部署AWS WAF解决方案来跨多个AWS账户管理AWS WAF规则.这些账户在AWS

Organizations中的不同OU下管理管理员必须能够根据需要从托管AWSWAF规则集中添加或删除账户或OU.管理 员还必须能够自动更新和修复所有账户中不合规的AWS WAF规则.哪种解决方案能够以最少的运营开销满足这些要 求？

1. 使用 AWS Firewall Manager 管理组织中跨账户的 AWS WAF 规则.使用 AWS Systems Manager Parameter Store 参数存储帐号和OU以管理根据需要更新参数以添加或删除账户或OU.使用Amazon EventBridge (Amazon

CloudWatch Events)规则来识别参数的任何更改并调用AWS Lambda函数来更新Firewall Manager管理账户中的安 全策略.

1. 部署组织范围的AWS Config规则，要求所选OU中的所有资源关联AWS WAF规则.通过使用AWS Lambda修 复不合规资源来部署自动修复操作通过使用AWS CloudFormation堆栈集部署AWS WAF规则以针对应用AWS

Config规则的相同OU.

1. 在组织的主账户中创建AWSWAF规则.使用AWS Lambda环境变量来存储帐号和要管理的OU.根据需要更新环 境变量以添加或删除帐户或OU.在成员账户中创建跨账户IAM角色.

通过在Lambda函数中使用AWS Security Token Service (AWS STS)代入角色，在成员账户中创建和更新AWS WAF 规则.

1. 使用 AWS Control Tower 管理组织中跨账户的 AWS WAF 规则 使用 AWS Key Management Service (AWS KMS) 存储帐号和OU进行管理.根据需要更新AWS KMS以添加或删除账户或OU.在成员账户中创建IAM用户允许主账 户中的AWS Control Tower使用访问密钥和秘密访问密钥在成员账户中创建和更新AWS WAF规则

答案:B

解析：

Q58.解决方案架构师必须分析公司的Amazon EC2实例和Amazon Elastic Block Store （Amazon EBS）卷以确定公司 是否有效地使用资源.该公司正在运行多个大型高内存EC2实例来托管以主动/被动配置部署的数据库集群.这些EC2 实例的利用率因使用数据库的应用程序而异，公司尚未确定模式.

解决方案架构师必须分析环境并根据调查结果釆取行动哪种解决方案最经济有效地满足这些要求？

1. 使用AWS Systems Manager Ops Center创建控制面板.为与EC2实例及其EBS卷关联的Amazon CloudWatch 指标配置可视化.定期査看仪表板，并确定使用模式.根据指标中的峰值调整EC2实例的大小.
2. 开启Amazon CloudWatch对EC2实例及其EBS卷的详细监控.创建和审查 基于指标的仪表板.确定使用模式.根据指标中的峰值调整EC2实例的大小.
3. 在每个EC2实例上安装Amazon CloudWatch代理.打开AWS Compute Optimizer.让它运行至少12小时.査看 Compute Optimizer的建议，并按照指示调整EC2实例的大小.
4. 注册AWS企业支持计jc'J. Turn on AWS Trusted Advisor.等待12小时 查看Trusted Advisor的建议，并按照指示调 整EC2实例的规模.

答案:C

解析：

C-当然，因为它的内存实例需要安装CW代理并配置内存指标-优化器将完成工作并分析并建议Ec2 EBS和EC2 实例的合理化-只需为每个EC2支付一个额外的指标.

A不正确OpsCenter正在识别实例故障等资源问题.不是为了成本优化D不符合成本效益

B-不会满足要求・没有内存数据也可以对所有EC2实例进行详细监控是昂贵的

Q59.一家公司在单个AWS区域中运行无服务器应用程序.该应用程序访问外部URL并从这些站点中提取元数据.该公 司使用 Amazon Simple Notification Service （Amazon SNS）主题将 URL 发布到 Amazon Simple.

队列服务（Amazon SQS）队列.AWS Lambda函数使用队列作为事件源并处理队列中的URL.结果保存到Amazon S3 存储桶中.该公司要处理其他地区的每个URL.以比较站点本地化URL可能存在的差异，必须从现有地区发布.结果必 须写入当前区域中的现有S3存储桶.哪些更改组合将产生满足这些要求的多区域部署？（选择两项）

1. 将带有Lambda函数的SQS队列部署到其他Region
2. 将各个Region中的SNS主题订阅到SQS队列中
3. 订阅各个Region中的SQS队列到SNS主题
4. 配置SQS队列发布URLs到每个Region的SNS主题
5. 将SNS主题和Lambda函数部署到其他区域

答案:AC

解析：

首先在每个区域创建SQS和Lambda,然后将SQS队列订阅到SNS主题（无需在每个区域创建另一个SNS主题） <https://docs.aws.amazon.com/AWSSimpleQueueService/latest>

/SQSDeveloperGuide/sqs-configure-subscribe-queue-sns-topic.html

该公司希望处理通过同•端点发布的URL,因此他们正在寻找具有跨区域交付但每个区域单独的SQS + Lambda的单 一 SNS.首先在每个区域创建SQS和Lambda,然后将SQS队列订阅到SNS主题（无需在每个区域创建另一个 SNS 主题）https://docs.aws.amazon.com/AWSSimpleQueueService/latest

/SQSDeveloperGuide/sqs-configure-subscribe-queue-sns-topic.html

Q60.一家视频流媒体公司最近推出了一款用于视频共享的移动应用程序.该应用程序将各种文件上传到us-east-1区域 中的Amazon S3存储桶.这些文件的大小范围从1 GB到10 GB.从澳大利亚访问该应用程序的用户体验到上传需要很 长时间.有时文件无法为这些用户完全上传.解决方案架构师必须针对这些上传改进应用程序的性能.

哪些解决方案将满足这些要求？（选择两项）

1. 在S3存储桶上启用S3TransferAcceleration.将应用配置为使用TransferAcceleration端点进行上传
2. 在每个区域配置一个S3存储桶来接收上传使用S3 Cross-Region Replication将文件复制到分发S3存储桶
3. 使用基于延迟的路由设置Amazon Route 53,以将上传路由到最近的S3存储桶区域.
4. 配置应用程序将视频文件分成块.使用分段上传将文件传输到Amazon S3
5. 修改应用程序，在上传前为文件添加随机前缀

答案:AD

解析：

Q61 -家公司将数据存储在多个Amazon DynamoDB表中.解决方案架构师必须使用无服务器架构，通过基于HTTPS 的简单API公开访问数据.该解决方案必须根据需求自动扩展.

哪些解决方案满足这些要求？(选择两项)

1. 创建一个Amazon API Gateway REST API,通过使用API直接集成到DynamoDB配置此API

网关的AWS集成类型.

1. 创建一个Amazon API Gateway HTTP API.®过使用API直接集成到DynamoDB配置此API

网关的AWS集成类型.

1. 创建一个Amazon API Gateway HTTPAPLifi过与从DynamoDB表返回数据的AWS Lambda函数的集成来配置 此 API.
2. 在AWS Global Accelerator中创建一个加速器.使用从DynamoDB表返回数据的AWS Lambda@Edge函数集成 配置此加速器.
3. 创建网络负载均衡器.配置侦听器规则以将请求转发到适当的AWS Lambda函数

答案:AC

解析：

Q62. •家零售公司在欧洲拥有本地数据中心该公司还拥有多区域AWS业务，包括eu-west-1和us-east-1区域.该公 司希望能够将网络流量从其本地基础设施路由到这两个区域中的任•区域中的VPC.公司还需要支持在这些区域的VPC 之间直接路由的流量.

网络上不能存在单点故障.

该公司己经从其本地数据中心创建了两个1 GbpsAWS Direct connect连接.每个连接都进入欧洲的一个单独的Direct Connect位置以实现高可用性.这两个位置分别命名为DX-A和DX-B,每个区域都有-个AWS Transit Gateway.配置 为路由该区域内的所有VPC间流量.

哪种解决方案可以满足这些要求？

1. 创建从DX・A连接到Direct Connect网关的私有MIF从DX-B创建私有VIF

连接到同一 Direct Connect 网关以实现高可用性.将 eu-west-1 和 us-east-1 transit gateways 与 Direct Connect gateway 美联起来 Peer the transit gateways each other to support cross-Region routing.

1. 创建从DX-A连接到直接连接网关的中转VIF.将eu-west-1 transit gateway与此Direct Connect网关相关联.创建 从DX-B连接到单独的Direct Connect网关的中转MF.

将us-east-n transit gateway与这个单独的Direct Connect网关相关联.对等直连网关

相互支持高可用性和跨区域路由.

1. 创建从DX-A连接到Direct Connect网关的中转VIF.从DX-B创建中转VIF

连接到同• Direct Connect网关以实现高可用性.将eu-west-1和us-east-1中转网关与此Direct Connect网关相关 联.配置Direct Connect网关以在中转网关之间路由流量.

1. 创建从DX-A连接到Direct Connect网关的中转VIF从DX-B创建中转VIF

连接到同• Direct Connect网关以实现高可用性.将eu-west-1和us-east-1中转网关与此Direct Connect网关相关 联.将中转网关相互对等以支持跨区域路由.

答案:D

解析：

A-不，VPC之间没有连接.

B-不，bcz DX网关不支持从一个VPN路由到另一个

(<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>) C -正确答案. <https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway>. html

D -不，如果中间没有Direct Connect网关,则不能将Direct Connect连接到Transit网关.

Q63. •家软件公司部署了 -个应用程序，该应用程序使用Amazon API Gateway、AWS Lambda函数和Amazon DynamoDB表来使用REST API.应用程序在PUT请求期间显示错误数量增加大多数PUT调用来自少数使用特定 API密钥进行身份验证的客户端.

一位解决方案架构师发现大量PUT请求来自•个客户端.API是非关键的，客户端可以容忍不成功调用的重试.但是，错 误会显示给客户并导致API声誉受损.

解决方案架构师应该推荐什么来改善客户体验？

1. 在客户端应用程序中实施具有指数退避和不规则变化的重试逻辑确保错误被捕获并使用描述性错误消息进行处理
2. 通过API网关级别的使用计划实施API节流确保客户端应用程序无错误地处理代码429回复
3. 开启API缓存以増强生产阶段的响应能力.运行10分钟的负载测试. 验证缓存容量是否适合工作负载.
4. 在Lambda函数级别实现预留并发，以提供在流量突然增加时所需的资源

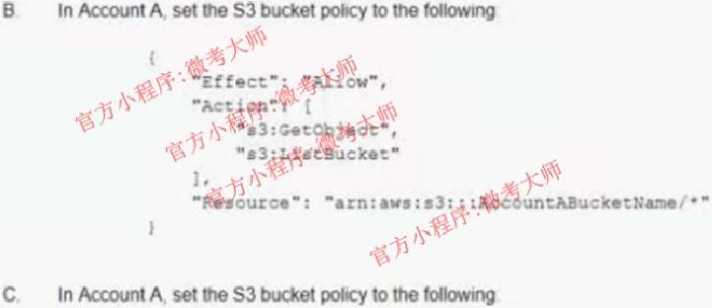
答案:A

解析:

Q64. •家零售公司需要向另-家公司提供•系列数据文件，这家公司是其业务合作伙伴.这些文件保存在属于零售公司的 账户A下的Amazon S3存储桶中.业务合作伙伴公司希望其IAM用户之一 User\_DataProcessor从其自己的AWS 账户（账户B）访问文件.

公司必须釆取哪些步骤组合才能使User\_DataProcessor可以成功访问S3存储桶？（选择两个.）

Turn on the crosmongm resource sharing (CORS) feature for me S3 bucket m Account A





\*«3:Li«tBucket\*

D In Account B. set the permissions of User\_DataProcess<x to the lollowmg



In Account B set the permissions of Usef.DataProcessoc to the toltowtng



1. 为账户A中的S3存储桶开启跨源资源共享(CORS)功能.
2. 在账户A中，将S3存储桶策略设置为以下内容：

{“效果”；“允许”，

“行动[

勺3：获取对象。

“g3：列表桶”

1.

“资源、warn:aws:s3:::AccountABucketName/\*M

}

1. 在账户A中，将S3存储柵策略设置为以下内容

{

“效果“允许"

“校长仁{

“AMS。"am： aws： iam：： AccountB：用户/用户数据处理

}，

“行动' [

ug3；获取対象)

ug3： LielBucket"

*]r*

D、 在 Account B 中，设置 User DataProcessor 的权限如下{ ”Effect":”AIlow”,

“行动[

Hs3：获取对象二

ug3； LigtBucketn

“资源”：Mam:aws:s3:::AccountABucketNanie/\*"

}

E,在帐户B中，将User\_DataProcessor的权限设置为以下内容:

{

"效果":"允许"，

“主要的”：(

“ANS”： "am:aws:iam::AccountB:user/User\_Dataprocessor”

).

“行动”：［

“S3：获取对象”，

••s3：列表桶”

］.

“资源”：［

“arn:aws:s3:::AccountABucketName/\*”

答案:CD

解析：

Q65.一家公司有一个组织，该组织在AWS Organizations中拥有许多AWS账户.解决方案架构师必须改进公司管理组 织中AWS账户的通用安全组规则的方式.

该公司在每个AWS账户的允许列表中都有一组通用的IPCIDR范围，以允许访问和来自公司的本地网络.每个帐户中 的开发人员负责将新的IPCIDR范围添加到他们的安全组中.安全团队有自己的AWS账户.目前，当对允许列表进行更 改时，安全团队会通知其他AWS账户的所有者.解决方案架构师必须设计一个解决方案，在所有账户中分配一组通用的 CIDR范围.

哪种解决方案能够以最少的运营开销满足这些要求？

1. 在安全团队的 AWS 账户中设置一个 Amazon Simple Notification Service (Amazon SNS)主题.

在每个AWS账户中部署一个AWSLambda函数.将Lambda函数配置为在每次SNS主题收到消息时运行.配置 Lambda函数以将IP地址作为输入并将其添加到

帐户.指示安全团队通过向其SNS主题发布消息来分发更改.

1. 在组织内的每个AWS账户中创建新的客户管理的前缀列表.使用所有内部CIDR范围填充每个帐户中的前缀列表. 通知每个AWS账户的所有者在其安全组的账户中允许新的客户管理的前缀列表ID.指示安全团队与每个AWS账户所 有者共享更新.
2. 在安全团队的AWS账户中创建一个新的客户管理的前缀列表.使用所有内部CIDR范围填充客户管理的前缀列表. 使用AWS Resource Access Manager与组织共享客户管理的前缀列表.通知每个AWS账户的所有者在其安全组中允 许新的客户管理的前綴列表ID.
3. 在组织中的每个账户中创建一个IAM角色.授予更新安全组的权限.

在安全团队的AWS账户中部署AWS Lambda函数.配置Lambda函数以将内部IP地址列表作为输入，在每个组织 账户中担任角色，并将IP地址列表添加到每个账户中的安全组.

答案:C

解析：

<https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html> 托管前缀列表是•组一个或多个 CIDR 块.您可以使用前缀列表来更轻松地配置和维护您的安全组和路由表.

<https://docs.aws.amazon.com/vpc/latest/userguide/sharing-managed-prefix-lists.html> 使用 AWS Resource Access Manager (AWS RAM),前缀列表的所有者可以与下列的：

AWS Organizations中其组织内部或外部的特定AWS账户AWS Organizations中其组织内部的组织单位AWS Organizations中的整个组织

Q66. •家公司开发了 •个Web应用程序.该公司在Application Load Balancer后面的•组Amazon EC2实例上托管 该应用程序.该公司希望改善应用程序的安全状况并计划使用AWSWAF WebACL.该解决方案不得对应用程序的合法流 量产生不利影响.

解决方案架构师应如何配置WebACL以满足这些要求？

1. 将WebACL规则的动作设置为Count Enable AWSWAF logging.分析误报请求.修改规则以避免任何误报.随着时间 的推移，将WebACL规则的操作从计数更改为阻止.
2. 在WebACL中仅使用基于速率的规则，并将限制限制设置得尽可能高.暂时阻止所有超过限制的请求.定义嵌套规则 以缩小速率跟踪范围
3. 将WebACL规则的动作设置为Block.在WebACL中仅使用AWS托管规则组.

通过将Amazon CloudWatch指标与AWS WAF采样请求或AWS WAF日志结合使用来评估规则组.

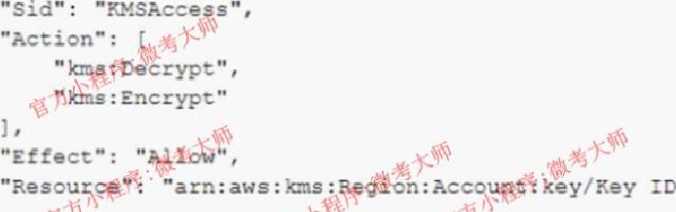
1. 在WebACL中仅使用自定义规则组，并将操作设置为允许.启用AWS WAF日志记录.

分析误报请求.修改规则以避免任何误报.随着时间的推移，将WebACL规则的操作从允许更改为阻止 答案:A

解析： 这道题是关于如何测试WebACL.先计数，再block <https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html> 此外，A 还包括 AWS 规则和 customer 规 则

Q67.解决方案架构师需要为将存储在新Amazon S3存储桶中的对象实施客户端加密机制.为此，解决方案架构师创建了 一个存储在 AWS Key Management Service (AWS KMS)中的 CMK.

解决方案架构师创建了以下IAM策略并将其附加到IAM角色： 在测试期间，解决方案架构师能够成功获取S3存储桶中的现有测试对象.但是，尝试上传新对象时出现错误消息.错误消 息指出该操作被禁止.



解决方案架构师必须将哪个操作添加到IAM策略才能满足所有要求？

1. kms:GenerateDataKey
2. kms:GetKeyPolicy
3. kms:GetPublicKey
4. 公里：标志

答案:A

解析：

Q68.-家大型移动游戏公司已成功将其所有本地基础设施迁移到AWS云.解决方案架构师正在审査环境，以确保它是根 据设计构建的，并且运行时符合Well-Architected Framework几种大型实例类型占成本的很大一部分.解决方案架构师发 现公司的开发人员正在启动新的Amazon EC2实例作为测试的一部分，并且开发人员没有使用适当的实例类型. 解决方案架构师必须实施一种控制机制来限制只有开发人员可以启动的实例类型.哪种解决方案可以满足这些要求？

1. 在AWS Config中创建所需实例类型的托管规则.使用允许的实例类型配置规则.

将规则附加到事件以在每次启动新的EC2实例时运行.

1. 在EC2控制台中，创建一个启动模板，指定允许的实例类型.将启动模板分配给开发人员的IAM账户
2. 创建一个新的IAM策略.指定允许的实例类型.将该策略附加到包含开发人员的IAM帐户的IAM组.
3. 使用EC2lmage Builder为开发者创建镜像管道，协助开发者创建黄金镜像.

答案:C

解析：

Q69.一家公司正在构建一个电子文件管理系统，用户可以在其中上传他们的文件.应用程序堆栈完全无服务器，在 eu-central-1区域的AWS上运行.该系统包括一个Web应用程序，该应用程序使用Amazon CloudFront分配以 Amazon S3作为源进行交付.Web应用程序与Amazon API Gateway区域端点通信.API网关API调用将元数据存储 在Amazon Aurora Serverless数据库中并将文档放入S3存储桶中的AWS Lambda函数.

该公司正在稳步发展，并已与其最大的客户完成了概念验证.该公司必须改善欧洲以外的延迟. 哪种行动组合将满足这些要求？（选择两项.）

1. 在 S3 存储桶上启用 S3 Transfer Acceleration.确保 Web 应用程序使用 Transfer Acceleration 签名 URL
2. 在AWS Global Accelerator中创建一个加速器.将加速器附加到CloudFront分配.
3. 将API网关区域端点更改为边缘优化端点
4. 在分布在世界各地的另外两个位置提供整个堆栈.在Aurora Serverless集群上使用全局数据库.
5. 在Lambda函数和Aurora Serverless数据库之冋添加一个Amazon RDS代理.

答案:AC

解析：

GA被排除在外，因为它不能指向CF如果我们使用CF也不需要GA-这个排除BD不需要太复杂 所以只剩下ACE-C肯定有帮助，S3传输可以帮助减少全球上传时间

Q70.一家健康保险公司将个人身份信息（PII）存储在Amazon S3存储桶中.该公司使用带有S3托管加密密钥 （SSE-S3）的服务器端加密来加密对象.

根据新要求，所有当前和未来

S3存储桶中的对象必须使用公司安全团队管理的密钥进行加密.S3存储桶未启用版本控制.

哪种解决方案可以满足这些要求？

1. 在S3bucket属性中，使用客户管理的密钥将默认加密更改为SSE-S3.

使用AWS CLI重新上传S3存储桶中的所有对象.设置S3存储桶策略以拒绝未加密的PutObject请求

1. 在S3bucket属性中，将默认加密更改为使用AWS KMS托管加密密钥(SSE-KMS)的服务器端加密.设置S3存储 桶策略以拒绝未加密的PutObject请求.使用AWS CLI重新上传S3存储桶中的所有对象
2. 在S3bucket属性中，将默认加密更改为使用AWS KMS托管加密密钥(SSE-KMS)的服务器端加密.设置S3存储 桶策略以自动加密GetObject和PutObject请求上的对象
3. 在S3bucket属性中，使用客户管理的密钥将默认加密更改为AES-256.

附加一个策略以拒绝任何访问S3存储桶的实体的未加密PutObject请求.使用AWS CLI重新上传所有对象 S3存储桶.

答案:B

解析：

Q71.-家公司正在AWS上构建软件即服务(SaaS)解决方案.该公司已在多个AWS区域和同一生产账户中部署了一 个集成了 AWS Lambda 的 Amazon API Gateway RESTAPL

该公司提供分层定价，使客户能够为每秒进行•定数量的API调用的容量付费.高级套餐每秒提供多达3,000次调用. 客户由唯•的API密钥识别.多个地区的-些高级客户报告说，他们在使用高峰期收到来自多个API方法的429Too Many Requests的错误响应.日志表明Lambda函数从未被调用.

这些客户的错误消息可能是什么原因造成的？

1. Lambda函数达到了并发限制.
2. Lambda函数达到并发的区域限制.
3. 公司达到了其API网关帐户每秒调用的限制.
4. 公司达到了其API网关默认的每方法每秒调用限制 答案:C

解析：

Q72l家公司使用AWS Organizations管理多个AWS账户.在根ou下，公司有两个OU： Research和DataOps. 由于法规要求，公司在组织中部署的所有资源都必须位于ap-northeast-1区域中.此外，公司在DataOpsOU中部署的 EC2实例必须使用预定义的实例类型列表.

解决方案架构师必须实施应用这些限制的解决方案.该解决方案必须最大限度地提高运营效率，并且必须最大限度地减少 日常维护.哪些步骤组合可以满足这些要求？(选择两项)

1. 在DataOps 0U下的 个帐户中创建•个IAM角色.在角色的内联策略中使用ec2:lnstanceType条件键来限制对 特定实例类型的访问.
2. 在根OU下的所有账户中创建一个IAM用户.在每个用户的内联策略中使用aws:RequestedRegion条件键来限制 对除ap-northeast-1以外的所有AWS区域的访问
3. 创建SCP使用aws:RequestedRegion条件键来限制对除ap-northeast-1之外的所有AWS区域的访问.将SCP 应用于根OU
4. 创建•个SCP.使用ec2:Region条件键限制对除ap-northeast-1之外的所有AWS区域的访问.将SCP应用于根 OU、DataOps 0U 和研究 0U
5. 创建一个SCP.使用ec2:lnstanceType条件键来限制对特定实例类型的访问.

将SCP应用于DataOps OU

答案:CE

解析：

Q73 -家公司在AWS上的VPC中托管图像处理服务.VPC跨越两个可用区.每个可用区包含一个公有子网和一个私 有子网.该服务在私有子网中的Amazon EC2实例上运行.公共子网中的Application Load Balancer位于服务前面.该服 务需要与Internet通信，并通过两个NAT网关进行通信.该服务使用Amazon S3进行图像存储. EC2实例每天从S3 存储桶中检索大约1 TB的数据.

该公司己将该服务提升为高度安全解决方案架构师必须尽可能减少云支岀，同时不影响服务的安全状况或增加持续运营 所花费的时间.

哪种解决方案可以满足这些要求？

1. 用NAT实例替换NAT网关.在VPC路由表中，创建从私有子网到NAT实例的路由
2. 将EC2实例移动到公共子网删除NAT网关.
3. 在VPC中设置S3网关VPC端点.将端点策略附加到端点以允许所需的

S3存储桶上的操作.

1. 将 Amazon Elastic File System (Amazon EFS)卷附加到 EC2 实例.在 EFS 卷上托管图像

答案:C

解析：

Q74. •家视频处理公司希望使用600 TB的压缩数据构建机器学习(ML)模型，这些压缩数据以数千个文件的形式存储 在公司的本地网络附加存储系统中.该公司没有必要的本地计算资源来进行ML实验，并希望使用AWS.

该公司需要在3周内完成向AWS的数据传输.数据传输将是•次性传输.数据在传输过程中必须加密. 公司网络连接实测上传速度为100Mbps.多个部门共享连接.

哪种解决方案能够最经济有效地满足这些要求？ 01-05-06

1. 使用AWS管理控制台订购多台AWS Snowball Edge Storage Optimized设备.使用目标S3存储桶配置设备.将数 据复制到设备.将设备运回AWS
2. 在公司位置和最近的AWS区域之间建立10GbpsAWS Direct Connect连接.通过VPN连接将数据传输到区域以 将数据存储在Amazon S3中

在本地网络附加存储和最近的AWS区域之间创建VPN连接.通过VPN连接传输数据

在本地部署AWS Storage Gateway文件网关.使用目标S3bucket配置文件网美将数据复制到文件网关

答案:A

解析：

Q75.一家公司在开发环境中的单个Windows Amazon EC2实例上运行内容管理应用程序该应用程序读取静态内容并将 其写入作为根设备附加到实例的2 TB Amazon Elastic Block Store (Amazon EBS)卷.该公司计划将该应用程序部署在 生产环境中，作为一个高度可用且容错的解决方案，该解决方案在跨多个可用区的至少三个EC2实例上运行.

解决方案架构师必须设计一个解决方案，将运行应用程序的所有实例连接到Active Directory域.该解决方案还必须实施 WindowsACLS来控制对文件内容的访问.应用程序必须始终在任何给定时间点在所有正在运行的实例上维护完全相同 的内容.

哪种解决方案能够以最少的管理开销满足这些要求？ 01-05-32

1. 创建一个Amazon Elastic File System (Amazon EFS)文件共享.创建一个扩展到三个可用区的Auto Scaling组，并 保持至少三个实例的大小.实现用户数据脚本安装应用，将实例加入AD域，挂载EFS文件共享
2. 从当前正在运行的EC2实例创建一个新的AMI.创建Amazon FSX for Lustre文件系统.创建一个扩展到三个可用区 的Auto Scaling组，并保持至少三个实例的大小.执行用户数据脚本将实例加入AD域并挂载FSX for Lustre文件系统
3. 为Windows文件服务器文件系统创建一个Amazon FSX.创建一个扩展到三个可用区的Auto Scaling组，并保持至 少三个实例的大小.实施用户数据脚本以安装应用程序并装载FSX for Windows File Server文件系统.执行无缝域加入以 将实例加入AD域
4. 从当前正在运行的Ec2实例创建一个新的AML创建Amazon Elastic File System (Amazon EFS)文件系统.创建一 个扩展到三个可用区的Auto Scaling组，并保持至少三个实例的大小.执行无缝域加入以将实例加入AD域

答案:C

解析:

Q76.一家数字营销公司拥有多个属于不同团队的AWS账户.创意团队在其AWS账户中使用Amazon S3存储桶来安 全地存储用作公司营销活动内容的图像和媒体文件.创意团队希望与战略团队共享S3存储桶，以便战略团队可以查看对 象解决方案架构师在战略账户中创建了 •个名为strategy\_reviewer的IAM角色.解决方案架构师还在Creative账户 中设置了自定义AWS Key Management Service (AWS KMS)密钥，并将该密钥与S3存储桶相关联.但是，当来自 Strategy账户的用户担任IAM角色并尝试访问S3存储桶中的对象时，他们会收到拒绝访问错误.解决方案架构师必须 确保Strategy账户中的用户可以访问S3存储桶.解决方案必须只为这些用户提供他们需要的最低权限.解决方案架构 师应该采取哪些步骤组合来满足这些要求？(选择三个.)

1. 创建•个包含S3存储桶读取权限的存储桶策略.将桶策略的委托人设置为Strategy账户的账户ID.
2. 更新strategy\_reviewer IAM角色以授予对S3存储桶的完全权限并授予对自定义KMS密钥的解密权限
3. 更新Creative账户中的自定义KMS密钥策略，以授予strategy\_reviewer IAM角色解密权限
4. 创建•个包含S3存储桶读取权限的存储桶策略.将存储桶策略的主体设置为匿名用户.
5. 更新Creative账户中的自定义KMS密钥策略，以向strategy\_reviewer IAM角色授予加密权限.
6. 更新strategy\_reviewer IAM角色以授予对S3存储桶的读取权庶并授予对自定义KMS密钥的解密权限.

答案:ACF

解析：

Q77.一家零售公司跨多个AWS区域在AWS上托管一个电子商务网站.该公司希望该网站在任何时候都可以在线购买 该网站将数据存储在Amazon RDS for MySQL数据库实例中.

哪种解决方案将为数据库提供最高的可用性？

1. 在Amazon RDS上配置自动备份.在中断的情况下，将自动备份提升为独立的数据库实例.将数据库流量定向到提升 的数据库实例.创建将提升的数据库实例作为其源的替换只读副本
2. 在Amazon RDS上配置全局表和只读副本.激活跨区域范围.在中断的情况下，使用AWS Lambda将只读副本从一 个区域复制到另一个区域
3. 在Amazon RDS上配置全局表和自动备份.在中断的情况下，使用AWS Lambda将只读副本从一个区域复制到另一 个区域
4. 在Amazon RDS上配置只读副本在发生中断的情况下，将跨区域只读副本提升为独立的数据库实例将数据库流量定 向到提升的数据库实例.创建将提升的数据库实例作为其源的替换只读副本 答案:D

解析：

Q78.对公司无服务器应用程序的外部审计掲示了授予过多权限的IAM策略.这些策略附加到公司的AWS Lambda执行 角色公司的数百个Lambda函数具有广泛的访问权限，例如对Amazon S3buckets和Amazon DynamoDB表的完全 访问权限.公司希望每个功能仅具有该功能完成其任务所需的最低权限.

解决方案架构师必须确定每个Lambda函数需要哪些权限.解决方案架构师应该怎么做才能以最少的工作量满足此要 求？

1. 设置Amazon CodeGuru以分析Lambda函数并搜索AWS API调用

每个Lambda函数所需的API调用和资源为每个Lambda函数创建新的IAM访问策略

审查新政策以确保它们符合公司的业务要求

1. 为AWS账户打开AWS CloudTrail日志记录.使用AWS身份和访问管理访问分析器来

根据CloudTrail日志中记录的活动生成IAM访问策略审查生成的策略以确保它们满足公司的业务需求

1. 为AWS账户打开AWSCloudrail日志记录.创建一个脚本来解析CloudTrail日志，搜索AWSAPI

按Lambda执行角色调用，并创建摘要报告查看报告创建IAM访问策略，提供 每个Lambda函数的权限更严格

1. 为AWS账户开启AWS CloudTrail日志记录将CloudTrail日志导出到Amazon S3使用Amazon EMR来 处理Amazon S3中的CloudTrail日志并生成每个执行角色使用的API调用和资源的报告

为每个角色创建新的IAM访问策略将生成的角色导出到S3bucket查看生成的策略

确保他们满足公司的业务要求

答案:B

解析：

Q79.一家公司推出了一项新政策，允许员工在使用VPN连接的情况下在家中远程工作.公司在多个AWS账戸中使用 VPCS托管内部应用程序目前，可以通过AWS站点到站点VPN连接从公司的本地办公室网络访问这些应用程序公 司\*要AWS账户中的VPC与VPCS建立了对等達接左其他AWS账户中.

解决方案架构师必须设计可扩展的AWS客户端VPN解决方案，供员工在家工作时使用

满足这些要求的最具成本效益的解决方案是什么？

1. 在每个AWS账户中创建一个客户端VPN终端节点.配置允许访问内部应用程序的所需路由
2. 在主AWS账户中创建客户端VPN端点配置允许访问内部的所需路由

应用程序

1. 在主AWS账户中创建一人客户端VPN端点提供一个连接到每个AWS的中转网关 account配置允许访问内部应用程序所需的路由
2. 在主AWS账户中创建客戸端VPN终端节点.在Client VPN终端节点和AWS Site-to-Site VPN之间建立连接

答案:B

解析：

Q80. •家公司正在AWS云中重构其本地订单处理平台.该平台包括一•个托管在•组虚拟机上的Web前端、将前端连接 到后端的RabbitMQ,以及•个运行容器化后端系统来处理订单的Kubernetes集群.该公司不想对应用程序进行任何重 大更改.哪种解决方案能够以最少的运营开销满足这些要求？ 2022032562

1. 创建Web服务器VM的AML创建一个使用AMI和应用程序负载均衡器的Amazon EC2Auto Scaling组.设置 Amazon MQ以替换本地消息队列.

配置 Amazon Elastic Kubernetes Service (Amazon EKS)以托管订单处理后端.

1. 创建自定义AWS Lambda运行时来模拟Web服务器环境.创建一个Amazon API Gateway API来替换前端Web 服务器，设置Amazon MQ来替换本地消息队列.配置Amazon Elastic Kubernetes Service (Amazon EKS)以托管订单 处理后端
2. 创建Web服务器VM的AML创建一个使用AMI和应用程序负载均衡器的Amazon EC2 Auto Scaling组.设置 Amazon MQ以替换本地消息队列.在一组不同的EC2实例上安装Kubernetes以托管订单处理后端
3. 创建Web服务器VM的AMI.创建•个使用AMI和应用程序负载均衡器的Amazon EC2 Auto Scaling组.设置 Amazon Simple Queue Service (Amazon SQS)队列以替换本地消息队列.配置 Amazon Elastic Kubernetes Service (Amazon EKS)以托管订单处理后端

答案:A

解析：

Q81.一家公司拥有数百个AWS账户.该公司最近实施了一个集中的内部流程，用于购买新的预留实例和修改现有的预留 实例.这个过程需要所有想要购买或修改预留实例的业务部门向专门的采购团队提交请求.以前，业务部门直接在各自的 AWS账户中自主购买或修改预留实例.解决方案架构师需要以最安全的方式实施新流程.解决方案架构师应该采取哪些步 骤组合来满足这些要求？(选择两个

1. 确保所有AWS账户都属于启用了所有功能的AWS Organizations中的组织.
2. 使用 AWS Config 报告拒绝访问 ec2:PurchaseReservedlnstancesOffering 操作和 ec2:ModifyReservedlnstances 操作的IAM策略附件.
3. 在每个 AWS 账户中，创建一个拒绝 ec2:PurchaseReservedlnstancesOffering 操作和 ec2:ModifyReservedInstances 操作的 IAM 策略.
4. 创建一个拒绝 ec2:PurchaseReservedinstancesOffering 操作和 ec2:ModifyReservedlnstances 操作的 SCP.将 SCP附加到组织的每个OU.
5. 确保所有AWS账户都是AWS Organizations中使用整合账单功能的组织的一部分.

答案:AE

解析：

Q82.一家公司想要迁移到AWS.该公司希望使用多账户结构，集中管理对所有账户和应用程序的访问.该公司还希望将流 量保持在专用网络上.登录时需要多因素身份验证(MFA),并将特定角色分配给用户组.

公司必须为开发、暂存、生产和共享网络创建单独的帐户.生产账户和共享网络账户必须连接到所有账户开发账户和临时 账户必须只能相互访问.解决方案架构师应该釆取哪些步骤组合来满足这些要求？(选择三项)

1. 使用AWS Control Tower部署登陆区环境.在AWS Organizations中注册账户并邀请现有账户加入生成的组织.
2. 在所有账户中启用AWS Security Hub以管理跨账户访问.通过AWS CloudTrail收集结果以强制MFA登录.
3. 在每个账户中创建中转网关和中转网关VPC附件.配置适当的路由表.
4. 设置并启用AWS单点登录.为现有帐户创建具有所需MFA的适当权限集.
5. 在所有账户中启用AWS Control Tower以管理账户之间的路由.通过AWS CloudTrail收集结果以强制MFA登录.
6. 创建IAM用户和组.为所有用户配置MFA.设置Amazon Cognito用户池和身份池以管理对账户和账户之间的访问

答案:ACE

解析:

Q83.解决方案架构师开发了 •个Web应用程序，该应用程序使用Amazon API Gateway区域终端节点和AWS Lambda函数.Web应用程序的消费者都靠近将部署应用程序的AWS区域.Lambda函数仅査询Amazon Aurora MySQL数据库.解决方案架构师已将数据库配置为具有三个只读副本.在测试过程中，应用程序不满足性能要求.在高负载 下，应用程序打开大量数据库连接.解决方案架构师必须提高应用程序的性能.

解决方案架构师应该采取哪些行动来满足这些要求？(选择两个.)

1. 使用Aurora数据库的集群端点.
2. 使用RDS Proxy设置连接池到Aurora数据库的读取端点.
3. 使用Lambda预置并发功能.
4. 将Lambda函数中打开数据库连接的代码移到事件处理程序之外.
5. 将API网关端点更改为边缘优化端点.

答案:BD

解析：

Q84. •家公司最近在AWS上部署了 •个应用程序.该应用程序使用Amazon DynamoDB.该公司测量了应用程序负载并 在DynamoDB表上配置了 RCU和WCU以匹配预期的峰值负载.峰值负载每周出现•次，持续4小时，是平均负载 的两倍.应用程序负载接近本周剩余时间的平均负载.访问模式包括对表的写入比对表的读取多得多.解决方案架构师需要 实施•个解决方案来最小化表的成本.

哪种解决方案可以满足这些要求？

1. 使用AWS Application Auto Scaling在高峰期增加容量.购买预留的RCU和WCU以匹配平均负载.
2. 为表配置按需容量模式.
3. 在表前配置DynamoDB Accelerator (DAX).减少预配置的读取容量以匹配表上的新峰值负载.
4. 在表前配置DynamoDB Accelerator (DAX).为表配置按需容量模式.

答案:A

解析:

Q85.一家公司想要使用第三方软件即服务(SaaS)应用程序.第三方SaaS应用程序通过多个API调用使用.第三方 SaaS应用程序也在VPC内的AWS上运行.

公司将从VPC内部使用第三方SaaS应用程序.公司有内部安全政策，要求使用不穿越互联网的专用连接.不允许从公 司VPC外部访问在公司VPC中运行的任何资源.所有权限必须符合最小特权原则.

哪个解决方案满足这些要求？

1. 创建•个AWS PrivateLink接口 VPC端点.将此端点连接到第三方SaaS应用程序提供的端点服务.创建安全组以 限制对端点的访问.

将安全组与端点相关联.

1. 在第三方SaaS应用程序和公司VPC之间创建AWS Site-to-Site VPN连接.配置网络ACL以限制跨VPN隧道 的访问.
2. 第三方SaaS应用与公司VPC建立VPC对等连接.

通过为对等连接添加所需的路由来更新路由表.

1. 创建AWS PrivateLink端点服务.请第三方SaaS提供商为此端点服务创建•个接口 VPC端点.将端点服务的权限 授予第三方SaaS提供商的特定帐户.

答案:A

解析：

<https://docs.aws.amazon.com/vpc/latest/privatelink/interface-endpoints.html>

您可以更改与接口端点的网络接口美联的安全组.安全组规则控制允许从VPC中的资源到终端节点网络接口的流量.

Q86.一家公司正在AWS云中运行Web应用程序.该应用程序包含在一组Amazon EC2实例上创建的动态内容.EC2 实例在配置为Application Load Balancer (ALB)的目标组的Auto Scaling组中运行.该公司正在使用Amazon

CloudFront分发益在全球范围内分发该应用程序.CloudFront分配使用ALB作为源.该公司将Amazon Route 53用于

DNS,并为CloudFront分配创建了 www.example.com的A记录.解决方案架构师必须配置应用程序，使其具有高可 用性和容错能力.

哪个解决方案满足这些要求？

1. 在不同的AWS区域预置完整的辅助应用程序部署.将Route 53Arecord更新为故障转移记录.添加两个CloudFront 分配作为值.创建Route 53健康检査
2. 在不同的AWS区域中配置ALB、Auto Scaling组和EC2实例.更新CloudFront分配，并为新的ALB创建第二 个源.为两个来源创建一个来源组.将一个原点配置为主要原点，将一个原点配置为次要原点.
3. 在不同的AWS区域配置Auto Scaling组和EC2实例.在ALB中为新的Auto Scaling组创建第二个目标.在ALB 上设置故障转移路由算法
4. 在不同的AWS区域预置完整的辅助应用程序部署.创建第二个CloudFront分配，并将新的应用程序设置添加为源. 创建一个AWS Global Accelerator加速器.将两个CloudFront分布添加为端点

答案:B

解析：

Q87.一家公司正在将其部分应用程序迁移到AWS.该公司希望在完成网络和安全策略后快速迁移和现代化应用程序.该公 司己在中央网络账户中设置了 AWS Direct Connect连接.该公司预计在不久的将来将拥有数百个AWS账尸和VPC.公 司网络必须能够无缝访问AWS上的资源，并且还必须能够与所有VPC进行通信该公司还希望通过其本地数据中心将 其云资源路由到互联网.

哪些步骤组合可以满足这些要求？(选择三个.)

1. 在中心账户中创建专线网关.在每个账户中，使用专线网关和每个虚拟私有网关的账户ID创建一个关联提议
2. 在中心网络账户中创建一个专线网关和一个中转网关，使用中转VIF将中转网关附加到专线网关上
3. 提供互联网网关将互联网网关附加到子网.允许互联网流量通过网关
4. 与其他账户共享transit gateway.将VPC附加到中转网关
5. 根据需要提供VPC对等
6. 仅提供私有子网.在中转网关和客户网关上打开必要的路由，以允许来自AWS的出站互联网流量流经在数据中心运行 的NAT服务

答案:BDF

解析：

Q88.应用程序在us-east-1区域中使用Amazon RDS for MySQL多可用区数据库实例在故障转移测试后，应用程序丢 失了与数据库的连接并且无法重新建立连接.应用程序重启后，应用程序重新建立连接.解决方案架构师必须实施解决方 案，以便应用程序无需重新启动即可重新建立与数据库的连接.

哪种解决方案可以满足这些要求？

1. 创建一个Amazon Aurora MySQL Serverless v1数据库实例将RDS数据库实例迁移到Aurora Serverless v1数 据库实例更新应用程序中的连接设置以指向Aurora读取器端点
2. 创建一个RDS代理.将现有RDS端点配置为目标更新应用程序中的连接设置以指向RDS代理端点
3. 创建一个双节点Amazon Aurora MySQL数据库集群.将RDS数据库实例迁移到Aurora数据库集群.创建RDS 代理.将现有RDS终结点配置为目标.更新应用程序中的连接设置以指向RDS代理端点
4. 创建一个 Amazon S3 桶.使用 AWS Database Migration Service (AWS DMS)将数据库导出到 Amazon S3.配置 Amazon Athena以将S3存储桶用作数据存储.为应用程序安装最新的开放式数据库连接(ODBC)驱动程序更新应用 程序中的连接设置以指向Athena端点

答案:B

解析:

Q89. •家公司拥有多个AWS账户-•个开发团队正在为云治理和补救流程构建•个自动化框架.自动化框架在集中式账 户中使用AWS Lambda函数.解袂方案架构师必须实施最低权限策略，允许Lambda函数在公司的每个AWS账户中 运行.哪些步骤组合可以满足这些要求？(选择两项)

1. 在集中账户中，创建一个将Lambda服务作为可信实体的IAM角色.添加内联策略以承担其他AWS账户的角色
2. 在其他AWS账尸中，创建一个具有最小权限的IAM角色.将集中账户的Lambda IAM角色添加为可信实体.
3. 在集中账户中，创建-个IAM角色，该角色具有•其他账户的角色作为可信实体.

提供最小权限

在其他AWS账户中，创建一个IAM角色，该角色有权限承担中心化账户的角色，将Lambda服务添加为可信实体 在其他AWS账户中，创建-个具有最小权限的IAM角色将Lambda服务添加为可信实体

答案:AB

解析;

Q90.某公司计划存储大量存档文档，并通过公司内网向员工提供这些文档.员工将通过连接到VPC的客户端VPN服务 来访问系统.数据不得向公众开放.公司存储的文档是保存在别处物理介质上的数据副本.请求的数量会很低可用性和检索 速度不是公司关心的问题.哪种解决方案能够以最低的成本满足这些要求？

1. 创建Amazon S3存储桶配置S3存储桶以默认使用S3 One Zone-Infrequent Access (S3 One Zone-IA)存储类 别.为网站托管配置S3存储桶.创建S3接曰端点.配置S3存储桶以仅允许通过该端点进行访问
2. 启动运行Web服务器的Amazon EC2实例.附加•个Amazon Elastic File System (Amazon EFS)文件系统以将 存档数据存储在EFS One Zone-Infrequent Access (EFS One Zone-IA)存储类中.配置实例安全组以仅允许从专用网络 访问
3. 启动运行Web服务器的Amazon EC2实例.附加Amazon Elastic Block Store (Amazon EBS)卷以存储存档数据 使用Cold HDD (sc1)卷类型.配置实例安全组以仅允许从专用网络访问
4. 创建•个Amazon S3桶.配置S3存储桶以默认使用S3 Glacier Deep Archive存储类配置用于网站托管的S3 存储桶.创建S3接口端点.配置S3存储桶以仅允许通过该端点进行访问

答案:D

解析：

Q91.一家公司已将其表单处理应用程序迁移到AWS.当用户与应用程序交互时，他们通过Web应用程序将扫描的表单 作为文件上传.数据库存储用户元数据和对食储在Amazon S3中的文件的引用.Web应用程序在Amazon EC2实例和 Amazon RDS for PostgreSQL 数据库上运行.

上传表单后，应用程序会通过Amazon Simple Notification Service (Amazon SNS)向团队发送通知.团队成员随后登录 并处理每个表单.团队成员在将信息输入另一个使用API的系统之前，对表单进行数据验证并提取相关数据.

解决方案架构师需要自动执行表单的手动处理.该解决方案必须提供准确的表单提取，最大限度地缩短上市时间，并最大 限度地减少长期运营开销.

哪种解决方案可以满足这些要求？

1. 开发自定义库以对表格执行光学字符识别(OCR).将库作为应用程序层部署到Amazon Elastic Kubemetes Service (Amazon EKS)集群.使用此层在上传表单时处理表单.将输出存储在Amazon S3中.通过将数据提取到Amazon DynamoDB表中来解析此输出.将数据提交到目标系统的API.在EC2实例上托管新的应用程序层.
2. 通过使用AWS Step Functions和AWS Lambda的应用程序层扩展系统.配置此层以使用在EC2实例上训练和托 管的人工智能和机器学习(AI/ML)模型，以便在上传表单时对表单执行光学字符识别(OCR).

将输出存储在Amazon S3中.通过提取应用层内所需的数据来解析此输出.将数据提交到目标系统的APL

1. 在EC2实例上托管一个新的应用层.使用此层调用托管在Amazon SageMaker中训练和托管的人工智能和机器学 习(AI/ML)模型的终端节点，以对表单执行光学字符识别(OCR).将输出存储在Amazon ElastiCache中.

通过提取应用层内所需的数据来解析此输出.将数据提交到日标系统的API.

1. 使用使用AWS Step Functions和AWS Lambda的成用程序层扩展系统.配置此层以使用Amazon Textract和 Amazon Comprehend在上传表单时对表单执行光学字符识别(OCR).将输出存储在Amazon S3中.通过提取应用层内 所需的数据来解析此输出.将数据提交到目标系统的API

答案:D

解析：

Q92. •家冒险公司在其移动应用程序上推出了 •项新功能.用户可以使用该功能随时上传他们的远足和漂流照片和视频. 照片和视频存储在S3存储桶中的Amazon S3标准存储中，并通过Amazon CloudFront提供.公司需要优化存储成本. 解决方案架构师发现大多数上传的照片和视频在30天后很少被访问.但是，有些上传的照片和视频在30天后被频繁访 问.解决方案架构师需要实施•种解决方案，以尽可能低的成本维持照片和视频的亳秒级检索可用性.

哪种解决方案可以满足这些要求？

1. 在S3存储桶上配置S3智能分层.
2. 配置S3生命周期策略以在30天后将图像对象和视频对象从S3 Standard转换为S3 Glacier Deep Archive.
3. 将 Amazon S3 替换为安装在 Amazon EC2 实例上的 Amazon Elastic File System (Amazon EFS)文件系统.
4. 添加Cache-Control:max-age标头到S3image对象和S3video对象.将标题设置为30天.

答案:D

解析：

Q93.-家公司有•个作为AWS Lambda函数托管的异步HTTP应用程序.公共Amazon API网关端点调用Lambda 函数Lambda函数和API网关终端节点位于us-east-1区域.解决方案架构师需要重新设计应用程序以支持故障转移 到另一个AWS区域.

哪种解决方案可以满足这些要求？

1. 在us-west-2区域创建API网关终端节点以将流量定向到us-east-1中的Lambda函数.配置Amazon Route 53 以使用故障转移路由策略为两个API网美终端节点路由流量.
2. 创建•个Amazon Simple Queue Service (Amazon SQS)队列.配置API网关以将流量定向到SQS队列而不是 Lambda函数.配置Lambda函数以从队列中拉取消息进行处理.
3. 将Lambda函数部署到us-west-2区域.在us-west-2中创建API网关终端节点以将流量定向到us-west-2中的 Lambda函数.配置AWS Global Accelerator和Application Load Balancer以管理跨两个API网关终端节点的流量.
4. 将Lambda函数和API网关端点部署到us-west-2区域.配置Amazon Route 53以使用故障转移路由策略为两个 API网关终端节点路由流量.

答案:D

解析：

Q94.一家公司在单个Amazon EC2实例上托管一个关键应用程序.该应用程序使用Amazon ElastiCache for Redis单 节点集群作为内存数据存储.该应用程序将Amazon RDS for MariaDB数据库实例用于关系数据库.为了使应用程序正常 运行，基础设施的每一部分都必须健康并且必须处于活动状态.解决方案架构师需要改进应用程序的体系结构，以便基础 架构可以自动从故障中恢复，停机时间尽可能短.哪些步骤组合可以满足这些要求？(选择三个.)

1. 使用Elastic Load Balancer在多个EC2实例之间分配流量.确保EC2实例是具有至少两个实例容量的Auto Scaling组的一部分.
2. 使用弹性负载均衡器在多个EC2实例之间分配流量.确保EC2实例配置为无限制模式.
3. 修改数据库实例以在同•可用区中创建只读副本.在故障场景中将只读副本提升为主数据库实例.
4. 修改数据库实例以创建跨两个可用区的多可用区部署.
5. 为ElastiCache for Redis集群创建•个复制组.将集群配置为使用至少具有两个实例容量的Auto Scaling组.
6. 为ElastiCache for Redis集群创建•个复制组.在集群上启用多可用区.

答案:ADE

解析：

Q95.一家公司在VPC的公共子网中的五个Amazon EC2实例上为移动应用程序托管一个基于REST的整体API.移 动客户端使用托管在Amazon Route 53上的域名连接到API.该公司使用所有EC2实例的IP地址创建了 Route 53 多值应答路由策略.最近，该应用程序因流量突然增加而不堪重负.该应用程序无法跟上流量.解决方案架构师需要实施解决 方案，以便应用程序能够处理新的和不断变化的负载.哪种解决方案能够以最少的运营开销满足这些要求？

1. 将API分成单独的AWS Lambda函数.使用Lambda集成为后端配置Amazon API Gateway RESTAPI.更新 Route 53记录以指向API网关API.
2. 容器化 API 逻辑.创建 Amazon Elastic Kubernetes Service (Amazon EKS)集群.使用 Amazon EC2 在集群中运行 容器.创建Kubernetes入口.更新Route 53记录以指向Kubernetes入口.
3. 创建一个Auto Scaling组.将所有EC2实例放在Auto Scaling组中.配置Auto Scaling组以执行基于CPU利用 率的扩展操作.创建一个AWS Lambda函数来响应Auto Scaling组更改并更新Route 53记录.
4. *在*API前面创建应用程序负载平衡器(ALB).将EC2实例移动到VPC中的私有子网.将EC2实例添加为ALB的 目标.更新Route 53记录以指向ALB.

答案:A

解析：

Q96.一家公司正在AWS云中运行应用程序.该应用程序收集大量非结构化数据并将其存储在Amazon S3存储桶中.S3 存储桶包含数TB的数据并使用S3标准存储类.数据的大小每天增加几千兆字节.公司需要査询和分析数据.公司不访问 超过1年的数据.但是，出于合规原因，公司必须无限期保留所有数据.哪种解决方案能够最经济有效地满足这些要求？

1. 使用S3 Select查询数据.创建S3Lifecycle策略以将超过1年的数据转换到S3 Glacier Deep Archive.
2. 使用Amazon Redshift Spectrum查询薮据.创建S3生命周期策略以将超过1年的数据转换到S3 Glacier Deep Archive.
3. 使用AWS Glue数据目录和Amazon Athena査询数据.创建S3生命周期策略以将超过1年的数据转换到S3 Glacier Deep Archive.
4. 使用Amazon Redshift Spectrum查询数据.创建S3生命周期策略以将超过1年的数据转换为S3智能分层

答案:C

解析：

Q97.一家视频处理公司有一个应用程序，可以从Amazon S3存储桶下载图像、处理图像、将转换后的图像存储在第二 个S3存储桶中，并在Amazon DynamoDB表中更新有关图像的元数据.该应用程序是用Nodejs编写的，并使用AWS Lambda函数运行.当新图像上传到Amazon S3时，将调用Lambda函数.该应用程序顺利运行了一段时间.但是，图像 的大小已显着增iJII. Lambda函数现在经常因超时错误而失败.函数超时设置为其最大值.解决方案架构师需要重构应用程 序的体系结构以防止调用失败.公司不想管理底层基础设施.解决方案架构师应该釆取哪些步骤组合来満足这些要求？

(选择两个.)

1. 通过构建包含应用程序代码的Docker映像来修改应用程序部署.

将镜像发布到 Amazon Elastic Container Registry (Amazon ECR)

1. 使用AWS Fargate的兼容类型创建新的Amazon Elastic Container Service (Amazon ECS)任务定义.配置任务定 义以使用Amazon Elastic Container Registry (Amazon ECR)中的新映像.调整Lambda函数以在新文件到达Amazon S3时使用ECS任务定义调用ECS任务
2. 创建具有并行状态的AWS Step Functions状态机以调用Lambda函数.

增加Lambda函数的配置并发

1. 使用Amazon EC2的兼容类型创建新的Amazon Elastic Container Service (Amazon ECS)任务定义.配置任务定义 以使用Amazon Elastic Container Registry (Amazon ECR)中的新映像.调整Lambda函数以松新文件到达Amazon S3时使用ECS任务定义调用ECS任务
2. 修改应用程序以在Amazon Elastic File System (Amazon EFS)上存储图像并将元数据存储在Amazon RDS数据库 实例上.调整Lambda函数以挂载EFS文件共享.

答案:AB

解析：

Q98.解决方案架构师正在审核•家公司的AWS Lambda函数的安全设置.Lambda函数从Amazon Aurora数据库中 检索最新的更改Lambda函数和数据库在同•个VPC中运行.Lambda环境变量为Lambda函数提供数据库凭证.

Lambda函数聚合数据并使数据在Amazon S3存储桶中可用，该存储桶配置为使用AWS KMS托管加密密钥 (SSE-KMS)进行服务器端加密.数据不得通过互联网传输.如果任何数据库凭据遭到破坏，公司需要一种能够最大限度地 减少破坏影响的解决方案.

解决方案架构师应该推荐什么来满足这些要求？

1. 在Aurora数据库集群上启用IAM数据库身份验证.更改Lambda函数的IAM角色以允许该函数使用IAM数据 库身份验证访问数据库.在VPC中为Amazon S3部署网关VPC终端节点.

在Aurora数据库集群上启用IAM数据库身份验证.更改IAM角色

1. Lambda函数允许函数使用IAM数据库身份验证访问数据库.

在数据传输期间对与Amazon S3的连接强制执行HTTPS.

1. 将数据库凭证保存在AWS Systems Manager Parameter Store中.在Parameter Store中的凭证上设置密码轮换.更 改Lambda函数的IAM角色以允许该函数访问Parameter Store.修改Lambda函数以从Parameter Store检索凭 证.

在VPC中为Amazon S3部署网关VPC终端节点.

1. 将数据库凭证保存在AWS Secrets Manager中.在Secrets Manager中的凭证上设置密码轮换.更改Lambda函数 的IAM角色以允许该函数访问Secrets Manager.修改Lambda函数以从Secrets Manager检索凭证.在数据传输期 间对与Amazon S3的连接强制执行HTTPS.

答案:A

解析：

它是无密码的，并为S3数据传输提供VPC网关，以避免通过Internet传输流量.

Q99.一家公司在Amazon EC2实例上运行传统的Web应用程序.公司需要将应用程序重构为在容器上运行的微服务. 应用程序的不同版本存在于两个不同的环境中：生产和测试.应用程序的负载是可变的，但最小负载和最大负载是已知的. 解决方案架构师需要使用无服务器架构设计更新的应用程序，以最大限度地降低操作复杂性.哪种解决方案能够最经济有 效地满足这些要求？

1. 将容器镜像作为函数上传到AWS Lambda.为关联的Lambda函数配置并发限制以处理预期的峰值负载.在Amazon API Gateway中配置两个单独的Lambda集成：一个用于生产，一个用于测试.
2. 将容器镜像上传到Amazon Elastic Container Registry (Amazon ECR).^用Fargate启动类型配置两个自动扩展的 Amazon Elastic Container Service (Amazon ECS)集群以处理预期负载.从ECR映像部署任务.配置两个单独的 Application Load Balancer以将流富定向到ECS集群.
3. 将容器镜像上传到Amazon Elastic Container Registry (Amazon ECR).使用Fargate启动类型配置两个自动扩展的 Amazon Elastic Kubernetes Service (Amazon EKS)集群以处理预期负载.从ECR映像部署任务.配置两个单独的 Application Load Balancer以将流量定向到EKS集群.
4. 将容器镜像上传到AWS Elastic Beanstalk.在Elastic Beanstalk中，为生产和测试创建单独的环境和部署.配置两个 单独的应用程序负载均衡器以将流量定向到Elastic Beanstalk部署

答案:B

解析：

Q100.使用AWSOrganizations的公司允许开发人员在AWS上进行试验.作为公司部署的着陆区的•部分，开发人员使 用他们公司的电子邮件地址来申请一个帐户.该公司希望确保开发人员不会推出昂贵的服务或不必要地运行服务.公司必 须为开发人员提供固定的每月预算，以限制他们的AWS成本.哪些步骤组合可以满足这些要求？(选择三个.)

1. 创建一个SCP以设置固定的每月帐户使用限制.将SCP应用到开发者帐户.
2. 使用AWS预算为每个开发人员的账户创建固定的每月预算，作为账户创建过程的一部分.

创建一个SCP以拒绝访问昂贵的服务和组件.将SCP应用到开发者帐户.

创建IAM策略以拒绝访问昂贵的服务和组件.将IAM策略应用于开发者账户.

1. 创建AWS预算警报操作以在达到预算金额时终止服务.

配置终止所有服务的动作.

1. 创建•个AWS预算警报操作以在达到预算金额时发送Amazon Simple Notification Service (Amazon SNS)通知.调 用AWS Lambda函数以终止所有服务.

答案:BCF

解析：

Q101.一家公司希望将其工作负载从本地迁移到AWS.工作负载在Linux和Windows上运行.该公司拥有大型本地基础 架构，其中包含托管大量应用程序的物理机和虚拟机.

公司必须捕获有关其本地工作负载的系统配置、系统性能、正在运行的进程和网络连接的详细信息.公司还必须将本地应 用程序分组以进行AWS迁移.公司需要有关Amazon EC2实例类型的建议，以便公司能够以最具成本效益的方式在 AWS上运行其工作负载.解决方案架构师应该采取哪些步骤组合来满足这些要求？(选择三个.)

1. 通过在物理机和VM上安装AWS Application Discovery Agent来评估现有应用程序.
2. 通过在物理机器和VM上安装AWS Systems Manager Agent来评估现有应用程序
3. 使用AWS Systems Manager Application Manager将服务器分组到应用程序中进行迁移.
4. 使用AWS Migration Hub将服务器分组到应用程序中进行迁移
5. 使用AWS Migration Hub生成推荐的实例类型和相关成本.
6. 将有关服务器大小的数据导入AWS Trusted Advisor,遵循成本优化的建议.

答案:ADE

解析：

Q102.出版公司的设计团队更新电子商务Web应用程序使用的图标和其他静态资产.该公司从托管在公司生产账户中的 Amazon S3存储桶中提供图标和资产.公司还使用设计团队成员可以访问的开发帐户

设计团队在开发账户中对静态资产进行测试后，设计团队需要将资产加载到生产账户中的S3 bucket中.解决方案架构师 必须为设计团队提供对生产帐户的访问权限，而不会将Web应用程序的其他部分暴露在不必要的更改风险之下

哪些步骤组合可以满足这些要求？

(选择三个.)

1. 在生产账户中,
2. 在开发帐户中,

创建一个新的 创建一个新的

IAM策略，允许对S3存储桶进行读写访问

IAM策略，允许对S3存储桶进行读写访问.

C.在生产账户中,

创建一个角色.将新策略附加到角色.将开发帐户定义为可信实体

D.在开发账户中,

创建一个角色.将新策略附加到角色.将生产帐户定义为可信实体.

E.在开发账户中,

执行 sts:AssumeRole 操作

创建一个包含设计团队所有IAM用户的组.将不同的IAM策略附加到组以允许对生产账户中的角色

F.在开发账户中，创建•个包含设计团队所有IAM用户的组.将不同的IAM策略附加到组中，以允许对开发账户中的 角色执行sts:AssumeRole操作

答案:ACE

解析:

Q103.•家公司拥有•个多层Web应用程序，该应用程序在Application Load Balancer (ALB)后面的•组Amazon EC2实例上运行.这些实例位于Auto Scaling组中.ALB和Auto Scaling组在备份AWS区域中复制.Auto Scaling组 的最小值和最大值设置为零.Amazon RDS多可用区数据库实例存储应用程序的数据.数据库实例在备份区域中有一个只 读副本应用程序使用Amazon Route 53记录向最终用户提供一个终端节点.

公司需要通过为应用程序提供自动故障转移到备份区域的能力，将其RTO减少到15分钟以内.公司没有足够多的预算 来实施主动-主动战略 解决方案架构师应该推荐什么来满足这些要求？

1. 使用基于延迟的路由策略重新配置应用程序的Route 53记录，以平衡两个ALBS之间的流量.在备份区域中创建一 个AWS Lambda函数以提升只读副本并修改Auto Scaling组值.创建基于主要区域中ALB的

HTTPCode\_Target\_5XX Count 指标的 Amazon CloudWatch 警报.配置 CloudWatch 警报以调用 Lambda 函数

1. 在备份if域中创证一个AWS Lambda函数以提升只读副本并修改Auto Scaling组值.使用运行状况检查配置 Route 53,以监控Web应用程序并在运行状况检查状态不佳时向Lambda函数发送Amazon Simple Notification Service (Amazon SNS)通知.使用故障转移策略更新应用程序的Route 53记录，该策略在发生健康检查失败时将流量 路由到备价区域中的ALB
2. 将备份区域中的Auto Scaling组配置为与主要区域中的Auto Scaling组具有相同的值.使用基于延迟的路由策略重 新配置应用程序的Route 53记录，以平衡两个ALBS之间的流量.删除只读副本.将只读副本替换为独立的RDS数据 库实例.通过使用快照和Amazon S3在RDS数据库实例之间配置Cross-Reaion Replication
3. 在AWS Global Accelerator中配置一个端点，将两个ALBS作为同等权重的目标.在备份区域中创建一个AWS Lambda函数以提升只读副本并修改Auto Scaling组值.为主要区域中的ALB创建基于

HTTPCode\_Target\_5XX\_Count 指标的 Amazon CloudWatch 警报.配置 CloudWatch 警报以调用 Lambda 函数.

答案:B

解析：

Q104.-家公司使用本地数据分析平台.该系统在公司数据中心的12台服务器上采用完全冗余配置，具有很高的可用性. 除了来自用户的•次性请求之外，系统还每小时和每天运行计划作业.计划的作业可能需要20分钟到2小时才能完成运 行并且具有严格的SLA.计划作业占系统使用率的65%.用户作业通常在5分钟内完成运行并且没有SLA.用户作业占 系统使用量的35%.在系统故障期间，计划的作业必须继续满足SLA.但是，用户作业可能会延迟.解决方案架构师需要将 系统迁移到Amazon EC2实例，并采用基于消费的模型来降低成本，而无需长期承诺.该解决方案必须保持高可用性并 且不得影响SLA.

哪种解决方案能够最经济有效地满足这些要求？

1. 将12个实例拆分到所选AWS区域中的两个可用区.在每个可用区中运行两个实例作为具有容量预留的按需实例.在 每个可用区中运行四个实例作为Spot实例.
2. 将12个实例拆分到所选AWS区域中的三个可用区.在其中一个可用区中，运行

所有四个实例都作为具有容量预留的按需实例.将其余实例作为Spot实例运行.

1. 将12个实例拆分到所选AWS区域中的三个可用区.使用Savings Plan在每个可用区中运行两个实例作为按需实 例.在每个可用区中运行两个实例作为Spot实例.
2. 将12个实例拆分到所选AWS区域中的三个可用区.在每个可用区中运行三个实例作为具有容量预留的按需实例.在 每个可用区中运行一个实例作为Spot实例.

答案:D

解析：

Q105,拥有多个AWS账户的公司正在使用AWS Organizations.公司的AWS账户托管VPC、Amazon EC2实例和容 器.

公司的合规团队在公司部署的每个VPC中都部署了安全工具.安全工具在EC2实例上运行，并将信息发送到专供合规 团队使用的AWS账户.公司已使用“costcenter”键和“compliance”值标记所有与合规性相关的资源.

该公司想要确定在EC2实例上运行的安全工具的成本，以便该公司可以向合规团队的AWS账户收费.成本计算必须尽 可能准确.

解决方案架构师应该怎么做才能满足这些要求？

1. 在组织的管理帐户中，激活成本中心用户定义标签.配置每月AWS成本和使用情况报告以保存到主账户中的 Amazon S3存储桶.

使用报告中的标签细分获取成本中心标记资源的总成本.

1. 在组织成员账户中，激活costCenter用户自定义标签.配置每月AWS Costand使用报告以保存到主账户中的

Amazon S3存储桶.

安排每月•次的AWS Lambda函数来检索报告并计算成本中心标记资源的总成本.

1. 在组织成员账户中，激活costCenter用户自定义标签.在主账户中，安排每月AWS成本和使用情况报告.使用报告中 的标签细分来计算成本中心标记资源的总成本.
2. 在AWS Trusted Advisor的组织视图中创建自定义报告.配置报告以生成合规团队AWS账户中成本中心标记资源的 月度账单摘要.

答案:C

解析：

Q106-家公司的解决方案架构师正在审查在AWS上运行的Web应用程序.该应用程序引用us-east-1区域中 Amazon S3存储桶中的静态资产.公司需要跨多个AWS区域的弹性.该公司已经在第二个区域中创建了一个S3存储 桶.哪种解决方案能够以最少的运营开销满足这些要求？

1. 配置应用程序将每个对象写入两个S3存储桶.通过对每个S3存储桶使用加权路由策略，设置一个包含记录集的 Amazon Route 53公共托管区域.配置应用程序以使用Route 53 DNS名称引用对象.
2. 创建一个AWS Lambda函数，将对象从us-east-1中的S3存储桶复制到第二个区域中的S3存储桶.每次将对象 写入us-east-1中的S3存储桶时调用Lambda函数.

使用包含两个S3存储桶作为源的源组设置Amazon Cloud Front分配.

1. 在us-east-1中的S3存储桶上配置复制以将对象复制到第二个区域中的S3存储桶.使用包含两个S3存储桶作 为源的源组设置Amazon CloudFront分配.
2. 在us-east-1中的S3存储桶上配置复制以将对象复制到第二个区域中的S3存储桶.如果需要故障转移，请更新应 用程序代码以从第二个区域中的S3存储桶加载S3对象.

答案:C

解析：

Q107.政府解决方案在2,000多个Amazon EC2实例组成的队列上运行.每个EC2实例都在安装了 AWS Systems Manager代理(SSM代理)的Windows Server操作系统上运行高度安全的软件.TCP/443入站端口对实例队列开放. 所有其他入站端曰均已关闭.目前，对端曰配置的任何更改都需要•个漫长的多级审查过程.哪种解决方案将提供安全访 问，以最少的管理开销在实例队列上运行脚本？

1. 为Puppet Enterprise配置AWS OpsWorks.使其连接到实例上的SSM代理使用Puppet堆栈管理脚本
2. 打开需要的端口.使用会话管理器管理实例队列，会话管理器是AWS Systems Manager的一项功能
3. 添加接曰端点和IAM角色.使用AWS Systems Manager的•项功能Run Command管理实例队列.
4. 打开端口 TCP/22并将脚本复制到每个实例上.使用脚本大规模管理实例

答案:B

解析:

Q108.-家公司最近将Web应用程序从本地数据中心迁移到AwS云,Web应用程序基础设施包括•个路由到应用程 序负载均衡器(ALB)的 Amazon CloudFront 分配，以及用于处理请求的 Amazon Elastic Container Service (Amazon

ECS).最近的安全审计表明，可以使用CloudFront和ALB端点访问Web应用程序.但是，公司要求Web应用程序必 须只能通过使用CloudFront端点访问.

哪种解决方案能够以最少的努力满足此要求？

1. 创建 个新的安全组并将其附加到CloudFront分配.更新ALB安全组入曰以仅允许来自CloudFront安全组的访问
2. 更新 ALB 安全组入口 以仅允许来自 com.amazonaws.global.cloudfront.origin-facing CloudFront 托管前綴列表的访 问
3. 为 Elastic Load Balancing 创建•个 com.amazonaws.region.elasticloadbalancing VPC 接口端点.将 ALB 方案从 面向Internet更新为内部
4. 从AWS提供的ip-rangesjson文档中提取CloudFront IP.更新ALB安全组入口以仅允许从CloudFront IP进行 访问

答案:C

*解析:*

Q109.一家公司开发了将Amazon API Gateway与区域终端节点结合使用的API. API调用使用API网关身份验证机 制的AWS Lambda函数.在设计审查之后，解决方案架构师确定了一组不需要公共访问的API.解决方案架构师必须设计 一个解决方案，使API集只能从VPC访问.所有API都需要由经过身份验证的用户调用.

哪种解决方案能够以最少的努力满足这些要求？

1. 创建•个内部应用程序负载均衡器（ALB）.创建•个目标组.选择要调用的Lambda函数.使用ALB DNS名称从 VPC调用API
2. 删除与API网关中的API关联的DNS条目.在Amazon Route 53中创建托管区域.在托管区域中创建CNAME 记录.使用CNAME记录更新API Gateway中的API.®用CNAME记录从VPC调用API
3. 在API网关中将API端点从区域更新为私有.在VPC中创建接口 VPC端点.创建资源策略，并将其附加到API. 使用VPC端点从VPC调用API
4. 在VPC内部署Lambda函数.配置一个EC2实例，并安装一个Apache服务器.

从Apache服务器调用Lambda函数.使用EC2实例的内部CNAME记录从VPC调用API

答案:C

解析：

Q110.一家公司在AWS上拥有其云基础设施.解决方案架构师需要将基础架构定义为代码.该基础设施目前部署在一个 AWS区域.该公司的业务扩展计划包括跨多个AWS账户在多个区域进行部署.解决方案架构师应该怎么做才能满足这 些要求？

1. 使用AWS CloudFormation模板.添加IAM策略以控制各种帐户.跨多个区域部署模板
2. 使用AWS Organizations.从主账户部署AWS CloudFormation模板.使用AWS Control Tower管理跨账户的部署
3. 使用 AWS Organizations 和 AWS CloudFormation StackSets.从具有必要 IAM 权限的账户部署 CloudFormation 模板
4. 将嵌套堆栈与AWS CloudFormation模板结合使用.使用嵌套堆栈更改区域

答案:A

解析：

Q111.一家零售公司己将其AWS账户构建为AWS Organizations中组织的一部分.该公司己设置整合账单并将其部门 映射到以下0U：财务销售、人力资源（HR）、市场营销和运营.每个0U都有多个AWS账户，每个账户对应一个部门 内的每个环境.这些环境是发展.测试.预生产•和生产.

人力资源部正在发布一个新系统，该系统将在3个月内推出.在准备.人力资源部门在其生产AWS账户中购买了多个预 留实例（RI）.人力资源部门将在此帐户上安装新的应用程序.HR部门希望确保其他部门不能共享RI折扣 哪种解决方案可以满足这些要求？

1. 在人力资源部门生产账户的AWS Billing and Cost Management控制台中，关闭RI共享
2. 从组织中删除人力资源部门的生产AWS账户.仅将帐户添加到合并账单配置
3. 在AWS Billing and Cost Management控制台中，使用组织的主账户为HR部门的生产AWS账户关闭RI共享
4. 在组织中创建一个SCP以限制对RI的访问.将SCP应用到其他部门的0U

答案:C

解析：

Q112.一家公司在AWS Organizations中有一个组织，其中包括多个AWS账户.每个账户都有一个VPC.在一个名为 Shared Services的账户中，有一个中转网关连接到Direct Connect网关，该网美提供对公司本地网络的访问.公司配置 AWS Resource Access Manager （AWS RAM）以将中转网关共享给组织中的所有账户.该公司已将所有VPC附加到中 转网关，以方便彼此之间的路由.

公司使用DNS服务器作为本地服务器.在本地和共享服务帐户VPC中有一对DNS服务器.公司发现公司在VPC中 启动的Amazon EC2实例无法解析地址私有本地域.哪种解决方案将允许所有VPC中的EC2实例解析木地地址’

1. 为共享服务账户VPC中的本地域定义一个Amazon Route 53 Resolver出站终端节点.将出站端点配置为使用本地 域的DNS服务器的IP地址.在DNS服务器上配置转发器以指向VPC的内部DNS解析器
2. 在共享服务账户VPC中为本地域创建一个Amazon Route 53私有托管区域.配置AWS Resource Access Manager (AWS RAM)以将托管区域共享给组织中的所有账户.将Route 53私有托管区域与每个VPC相关联
3. 为共享服务账户VPC中的本地域定义一个Amazon Route 53 Resolver出站终端节点.将出站端点配置为使用本地 域的 DNS 服务器的 IP 地址.配置 AWS Resource Access Manager (AWS RAM)以将 Route 53 Resolver 规则共享 给组织中的所有账户.将Route 53 Resolver规则与每个VPC相关联
4. 为共享服务账户VPC中的本地域定义一个Amazon Route 53 Resolver入站端点.将入站端点配置为使用本地域的 DNS 服务器的 IP 地址.配置 AWS Resource Access Manager (AWS RAM)以将 Route 53 Resolver 规则共享给组织 中的所有账户.将Route 53 Resolver规则与每个VPC相关联

答案:C

解析：

Q113. •家公司正在AWS云中运行应用程序.公司的安全团队必须批准所有新IAM用户的创建.创建新的IAM用户时， 必须自动删除该用户的所有访问权限.然后，安全团队必须收到批准用户的通知.该公司在AWS账户中拥有多区域AWS CloudTrail 跟踪.

哪种步骤组合可以满足这些要求？(选择三项.)

1. 创建一个 Amazon EventBridge 规则.定义一个模式，其中 detail-type 值设置为 AWS API Call via CloudTrail, eventName 为 Create User
2. 配置 CloudTrail 以将 CreateUser 事件的通知发送到 Amazon Simple Notification Service (Amazon SNS)主题
3. 使用AWS Fargate技术调用在Amazon Elastic Container Service (Amazon ECS)中运行的容器以删除謗问权限
4. 调用AWS Step Functions状态机以删除访问权限
5. 使用 Amazon Simple Notification Service(Amazon SNS)通知安全团队
6. 使用Amazon Pinpoint通知安金团队

答案:ADE

解析：

Q114.一家国际快递公司在AWS上托管了一个快递管理系统.司机使用系统上传交货确认.确认包括收件人的签名或收件 人的包裹照片.司机的手持设备通过FTP将签名和照片上传到单个Amazon EC2实例.每个手持设备根据登录用户在目录 中保存一个文件，文件名与交付编号匹配.在查询中央数据库以提取交付信息后，EC2实例将元数据添加到文件中.然后 将文件放置在Amazon S3中进行存档.随着公司的扩张，司机报告系统拒绝连接.FTP服务器由于连接中断和内存问题 而出现问题.针对这些问题，系统工程师安排了一个cron任务，每30分钟重启一次EC2实例.计费团队报告说，文件并 不总是在存档中，而且中央系统并不总是更新.解决方案架构师需要设计一个最大化可扩展性的解决方案，以确保存档始 终接收文件并且系统始终得到更新.手持设备无法修改，因此公司无法部署新的应用程序.

哪种解决方案可以满足这些要求？

1. 创建现有 EC2 实例的 AMI.在 Application Load Balancer 后面创建 EC2 实例的 Auto Scaling 组.将 Auto Scaling 组配置为至少具有三个实例
2. 使用 AWS Transfer Family 创建•个 FTP 服务器，将文件放置在 Amazon Elastic File System (Amazon EFS)中. 将EFS卷挂载到现有的EC2实例.将EC2实例指向文件处理的新路径
3. 使用 AWS Transfer Family 创建一个 FTP 服务器，将文件放在 Amazon S3 中.通过 Amazon Simple Notification Service (Amazon SNS)使用S3事件通知来调用AWS Lambda函数.配置Lambda函数以添加元数蠢并更新交付系 统
4. 更新手持设备以将文件直接放在Amazon S3中.通过Amazon Simple Queue Service (Amazon SQS)使用S3事 件通知来调用AWSLambda函数,配置Lambda函数以添加元数据并更新交付系统

答案:C

解析：

Q115.某公司正在运行一个关键应用程序，该应用程序使用Amazon RDS for MySQL数据库存储数据.RDS数据库实例 以多可用区模式部署.

最近的RDS数据库故障转移测试导致应用程序中断40秒.解决方案架构师需要设计一个解决方案，将中断时间减少到 20秒以内.解决方案架构师应该采取哪些步骤组合来满足这些要求？（选择三项.）

1. 数据库前端使用 Amazon ElastiCache for Memcached
2. 数据库前使用 Amazon ElastiCache for Redis
3. 数据库前使用RDS Proxy
4. 将数据库迁移到Amazon Aurora MySQL
5. 创建一个Amazon Aurora副本
6. 创建RDS for MySQL只读副本

答案:CDE

解析：

Q116.-家公司使用AWS Organizations在AWS云中进行多账户设置.该公司使用AWS Control Tower进行治理，并 使用AWS Transit Gateway进行跨账户的VPC连接.在一个AWS应用程序帐户中，公司的应用程序团队部署了一个 使用AWS Lambda和Amazon RDS的Web应用程序.公司的数据库管理员有•个单独的DBA账户，并使用该账户集 中管理整个组织的所有数据库.数据库管理员使用部署在DBA账户中的Amazon EC2实例访问部署在应用程序账户中的 RDS数据库.

应用程序团队已将数据库凭证作为机密存储在应用程序账户的AWS Secrets Manager中.应用程序团队正在与数据库管 理员手动共享机密.这些机密由应用程序账户中Secrets Manager的默认AWS托管密钥加密.解决方案架构师需要实施 一种解决方案，使数据库管理员能够访问数据库并消除手动共享机密的需要.

哪种解决方案可以满足这些要求？

1. 使用AWS Resource Access Manager （AWS RAM）与DBA账户共享来自应用程序账户的秘密.在DBA账户中，创 建•个名为DBA-Admin的IAM角色.授予该角色访问共享机密所需的权限.将DBA-Admin角色附加到EC2实例以 访问跨账户机密
2. 在应用程序帐户中，创建一个名为DBA-Secret的IAM角色.授予角色访问机密所需的权限.在DBA账户中，创建 一个名为DBA-Admin的IAM角色.

授予DBA-Admin角色所需的权限，以承担应用程序帐户中的DBA-Secret角色.将DBA-Admin角色附加到EC2实例 以访问跨账户机密

1. 在DBA帐户中，创建•个名为DBA-Admin的IAM角色.授予该角色访问应用程序帐户中的秘密和默认AWS托管 密钥所需的权限.在应用程序帐户中，将基于资源的策略附加到密钥以允许从DBA怅户访问将DBA-Admin角色附加 到EC2实例以访问跨帐户机密
2. 在DBA帐户中，创建一个名为DBA-Admin的IAM角色.授予该角色访问应用程序帐户中的机密所需的权限.将 SCP附加到应用程序帐户以允许从DBA帐户访问机密.将DBA-Admin角色附加到EC2实例以访问跨账户密码

答案:D

解析:

Q117.一家公司计划将其关键业务应用程序从本地数据中心迁移到AWS.该公司在本地安装了 Microsoft SQL Server Always On群集.该公司想要迁移到AWS托管数据库服务.解决方案架构师必须设计AWS上的异构数据库迁移 哪种解决方案可以满足这些要求？

1. 使用备份和恢复实用程序将SQL Server数据库迁移到Amazon RDS for MySQL
2. 使用 AWS Snowball Edge Storage Optimized 设备将数据传输到 Amazon S3.为 MySQL 设置 Amazon RDS 使用S3与SQL Server功能的集成，例如BULK INSERT
3. 使用 AWS Schema Conversion Tool 将数据库模式转换为 Amazon RDS for MySQL.然后使用 AWS

数据库迁移服务（AWS DMS）将数据从本地数据库迁移到Amazon RDS

1. 使用AWS DataSync通过网络在本地存储和Amazon S3之间迁移数据.

为MySQL设置Amazon RDS.f$用S3与SQL Server功能的集成.比如批量插入

答案:C

Q118.一家公司正在AWS云中运行应用程序.该应用程序在Amazon Elastic Container Service (Amazon ECS)集群中 的容器上运行.ECS任务使用Fargate启动类型.该应用程序的数据是关系数据，存储在Amazon Aurora MySQL中.为 满足监管要求，应用程序必须能够在发生应用程序故障时恢复到单独的AWS区域.在发生故障的情况下，不会丢失任何 数据.

哪种解决方案能够以最少的运营开销满足这些要求？

1. 在不同区域提供Aurora副本
2. 设置AWS DataSync以将数据连续复制到不同区域
3. 设置AWS Database Migration Service (AWS DMS)以将数据连续复制到不同区域
4. 使用 Amazon Data Lifecycle Manager (Amazon DLM)每 5 分钟安排一次快照

答案:A

解析：

Q119.-家公司部署了 Amazon Connect联络中心.联络中心代理报告了大量计算机生成的呼叫.公司担心这些呼叫对成 本和生产力的影响.该公司需要•种解决方案，允许座席将呼叫标记为垃圾邮件，并在未来自动阻止号码转到座席. 满足这些要求的最有效的运营解决方案是什么？

A.通过添加一个标志调用按钮来自定义联系人控制面板(CCP),该按钮将调用调用UpdateContactAttributesAPI的 AWS Lambda 函数.

使用Amazon DynamoDB表存储垃圾邮件号码.修改联系流以査找更新的属性并使用Lambda函数读取和写入 DynamoDB 表

1. 使用Contact Lens for Amazon Connect规则查找垃圾电话.使用Amazon DynamoDB表存储垃圾邮件号码.修改联 系流以查找规则并调用AWS Lambda函数来读取和写入DynamoDB表
2. 使用Amazon DynamoDB表存储垃圾邮件号码.创建-个快速连接，代理可以将垃圾邮件呼叫从联系人控制面板 (CCP)转移到该连接.修改快速连接联系流以调用AWS Lambda函数写入DynamoDB*表*
3. 修改初始联系流程以请求呼叫者输入.如果代理没有收到输入，代理应该将呼叫者标记为垃圾邮件.使用亚马逊 用于存储垃圾邮件号码的DynamoDB表.使用AWS Lambda函数读取和写入DynamoDB表

答案:C

解析：

Q120.公司由两个独立的业务部门组成.每个业务部门在AWS Organizations中的单个组织内都有自己的AWS账户.业 务部门经常相互共享敏感文件.为了方便共享，该公司在每个账户中创建了一个Amazon S3存储桶，并在S3存储桶之 间配置了双向复制.S3存储桶有数百万个对象最近，一项安全审计发现两个S3存储桶都没有启用静态加密.公司政策 要求所有文档必须以静态加密方式存储.公司希望使用Amazon S3托管加密密钥(SSE-S3)实施服务器端加密满足这 些要求的最高效的运营解决方案是什么？

1. 在两个S3存储桶上打开SSE-S3.使用S3批量操作复制和加密同•位置的对象
2. 在每个账户中创建一个AWS Key Management Service (AWS KMS)密钥.使用该AWS账户中相应的KMS密钥， 在每个S3存储桶上使用AWS KMS密钥(SSE-KMS)打开服务器端加密.在AWS CLI中使用S3复制命令加密现 有对象
3. 在两个S3存储桶上打开SSE-S3.在AWS CLI中使用S3复制命令加密现有对象
4. 在每个账户中创建一个AWS Key Management Service (AWS KMS)密钥.通过使用该AWS账户中的相应KMS 密钥，在每个S3存储桶上启用使用AWS KMS密钥(SSE-KMS)的服务器端加密.使用S3批量操作将对象复制到同 一位置

答案:A

解析：

Q121 -家制造公司开发了一种收集工厂车间设备遥测数据的流程.该公司使用AWS Control Tower.该公司还使用AWS CloudFormation 堆栈通过 Amazon Elastic Container Service (Amazon ECS)和 Amazon CloudWatch 中的一组容器 为每个工厂位置预置新的VPC.

该公司现在正在收购另一家拥有地理位置偏远工厂的制造公司.公司希望对这些工厂进行现代化改造.其中一项任务是应 用相同的遥测收集过程.将设备直接连接到AWS网络中的服务所导致的网络延迟非常高，这会影响可氣性.

公司如何将新工厂整合到现有架构中？

1. 使用AWS Control Tower创建新0U来为新工厂添加新账户.将ECS容器和CloudWatch部署到账户中
2. 为新收购的植物申请AWS Snowball Edge设备.将设备连接到AwS loT Core并通过AWS loT Core注册所有工厂 车间设备.将设备映射到现有VPC并将设备连接到ECS容器
3. 在新收购的工厂中申请并安装AWS Outposts服务器.在Outposts服务器中，使用CloudFormation堆栈配置所需 的VPC和ECS容器以连接到设备.

连接到AWS区域中的CloudWatch

1. 使用Amazon EC2专用实例.使用CloudFormation堆栈供应所需的VPC和ECS容器.连接到AWS区域中的 CloudWatch

答案:C

解析：

Q122 -家金融公司正计划将其Web应用程序从本地迁移到AWS.该公司使用第三方安全工具来监控应用程序的入站 流量.该公司在过去15年一直使用该安全工具，但该工具的供应商没有可用的云解决方案.该公司的安全团队担心如何将 安全工具与AWS技术集成.该公司计划将应用程序迁移部署到Amazon EC2实例上的AWS.EC2实例将在专用VPC 中的Auto Scaling组中运行.公司需要使用安全工具来检査所有进出VPC的数据包.此检査必须实时进行，并且不得影 响应用程序的性能.解决方案架构师必须在AWS上设计一个在AWS区域内高度可用的目标架构.

解决方案架构师应该采取哪些步骤组合来满足这些要求？(选择两项)

1. 在现有VPC中的新Auto Scaling组中的EC2实例上部署安全工具
2. 在网络负载均衡器后面部署Web应用程序
3. 在安全工具实例前部署应用程序负载均衡器
4. 为每个可用区配置网关负载均衡器以将流量重定向到安全工具
5. 提供transit gateway方便VPC之间的通信

答案:CD

解析：

Q123.一家公司在eu-west-1区域运行其应用程序，并为其每个环境拥有一个帐户：

开发、测试和生产.通过使用有状态的Amazon EC2实例和Amazon RDS for MySQL数据库，所有环境每周7天、每 天24小时不间断运行.数据库的大小在500 GB到800 GB之间.

开发团队和测试团队在工作日的工作时间工作，但生产环境每周7天、每天24小时不间断运行.公司希望降低成本.所 有资源都标有以开发、测试或生产为键的环境标签.解决方案架构师应该如何以最少的运营努力降低成本？

1. 创建每天运行一次的Amazon EventBridge规则.配置规则以调用一个AWS Lambda函数，该函数根据标签、日期 和时间启动或停止实例
2. 创建一个在每个工作日晚上运行的Amazon EventBridge规则.配置规则以调用根据标签停止实例的AWS Lambda 函数.创建在每个工作日早上运行的第二个EventBridge规则.配置第二条规则以调用另一个Lambda函数，该函数根据 标签启动实例
3. 创建一个在每个工作日晚上运行的Amazon EventBridge规则.配置规则以调用AWS Lambda函数，该函数根据标 签终止实例.创建在每个工作日早上运行的第二个EventBridge规则.配置第二条规则以调用另一个Lambda函数，该函 数根据标签从上次备份中恢复实例
4. 创建一个每小时运行一次的Amazon EventBridge规则.配置规则以调用一个AWS Lambda函数，该函数根据标签、 日期和时间从上次备份中终止或恢复实例 答案:B

Q124.一家金融服务公司从其信用卡服务合作伙伴处收到定期数据馈送.每15分钟以明文形式发送大约5,000条记录. 通过HTTPS直接传送到具有服务器端加密的Amazon S3存储桶中.此Feed包含敏感的信用卡主帐号（PAN）数据. 公司需要在将数据发送到另一个S3存储桶以进行额外的内部处理之前自动屏蔽PAN.公司还需要删除和合并特定字 段，然后将记录转换为JSON格式.此外，将来可能会添加额外的提要，因此任何设计都需要易于扩展.

哪些解决方案将满足这些要求？

1. 在文件传输时调用AWS Lambda函数，提取每条记录并将其写入Amazon SQS队列.当新消息到达SQS队列时调 用另一个Lambda函数来处理记录，将结果写入Amazon S3中的临时位置.一旦SQS队列为空，调用最终的Lambda 函数将记录转换为JSON格式并将结果发送到另一个S3存储桶进行内部处理
2. 在文件传输时调用AWS Lambda函数，提取每条记录并将其写入Amazon SQS队列.配置AWS Fargate容器应用 程序以在SQS队列包含消息时自动扩展到单个实例.让应用程序处理每条记录，并将记录转换为JSON格式.当队列为 空时，将结果发送到另一个S3存储桶进行内部处理并缩小AWS Fargate实例
3. 创建一个AWS Glue爬虫和基于数据馈送格式的自定义分类器，并构建一个表定义来匹配.在文件传输时调用AWS Lambda函数以启动AWS Glue ETL作业以根据处理和转换要求转换整个记录.将输出格式定义为JSON.完成后，让 ETL作业将结果发送到另一个S3存储桶进行内部处理
4. 根据数据馈送格式创建一个AWS Glue爬虫和自定义分类器，并构建一个表定义来匹配.对文件传输执行Amazon Athena査询以启动Amazon EMR ETL作业以根据处理和转换要求转换整个记录.将输出格式定义为JSON.完成后，将 结果发送到另一个S3存储桶进行内部处理并缩减EMR集群.

答案:C

解析：

您可以使用Glue爬网程序用表填充AWS Glue数据目录.可以触发Lambda函数 当对象创建事件发生时使用S3事件通知.然后Lambda函数将触发Glue ETL作业 转换记录以屏蔽敏感数据并将输出格式修改为JSON.这个解决方案满足所有

要求.

Q125.•家公司正在使用Auto Scaling组中的Amazon EC2实例在AWS云中处理视频.处理•个视频需要30分钟 多个EC2实例根据Amazon Simple Queue Service （Amazon SQS）队列中的视频数量进行扩展和扩展.该公司己使用 指定目标死信队列和1的maxReceiveCount的重新驱动策略配置SQS队列.该公司己将SQS队列的可见性超时设 置为1小时.该公司设置了一个Amazon CloudWatch警报，当死信队列中有消息时通知开发团队.

一夭中有好几次，开发团队收到消息在死信队列中并且视频没有得到正确处理的通知.调查发现应用程序日志中没有错误 公司如何解决这个问题？

1. 为EC2实例开启终止保护
2. 将SQS队列的可见性超时更新为3小时
3. 在处理过程中为实例配置缩容保护
4. 更新「edrive策略并将maxReceiveCount设置为0

答案:C

解析:

作为旁白：

AWS Certified Solutions Architect Professional是AWS的顶级认证.非技术人员很难把每道题看几个小时，耗费大量的时 间和精力，从而影响自己的工作.如果非技术人员有需要联系微信客服：ANYPASS.我们会帮你轻松通过（当然如果技术 人员有需要也可以联系，祝大家考试顺利！！

Q126.解决方案架构师正在调查公司无法在Amazon Workspaces中建立新会话的问题.初步分析表明该问题涉及用户 配置文件.Amazon Workspaces环境配置为使用Amazon FSx for Windows File Server作为配置文件共享存储.FSx for Windows File Server文件系统配置有10 TB的存储空冋.解决方案架构师发现文件系统己达到其最大容量.解决方案架 构师必须确保用户可以重新获得访问权限.解决方案还必须防止问题再次发生.

哪种解决方案可以满足这些要求？

1. 删除叮的用户配置文件以创建空间.将用户配置文件迁移到Amazon FSx for Lustre文件系统
2. 使用update-file-system命令增加容量.实施监控可用空冋的Amazon CloudWatch指标.使用Amazon EventBridge 调用AWS Lambda函数以根据需要增加容量.
3. 使用Amazon CloudWatch中的FreeStorageCapacity指标监控文件系统.根据需要使用AWS Step Functions增 加容量
4. 删除旧的用户配置文件以创建空冋.为Windows文件服务器文件系统创建一个额外的FSx.

为50%的用户更新用户配置文件重定向以使用新文件系统

答案:B

解析：

Q127.某公司为其NAT网关启用了 VPC流日志.对于来自公共IP地址198.51.100.2并发往私有Amazon EC2实 例的入站流量，该公司发现Action = ACCEPT.

解决方案架构师必须确定流量是否代表来自Internet的未经请求的入站连接.VPC CIDR块的前两个八位字节是 203.0.解决方案架构师应该釆取哪些步骤来满足这些要求？

1. 打开AWS CloudTrail控制台.选择包含NAT网关弹性网口和私有实例弹性网口的日志组.运行查询以将目标地址设置 为“like 203.0”并将源地址设置为“like 198.51.100.2”进行过滤.运行stats命令过滤源地址和目的地址传输的字节总和
2. 打开Amazon CloudWatch控制台.选择包含NAT网关弹性网口和私有实例弹性网口的日志组.运行查询以将目标地址 设置为“like 203.0”并将源地址设置为“like 198.51.100.2"进行过滤.运行stats命令过滤源地址和目的地址传输的字节总和
3. 打开AWS CloudTrail控制台.选择包含NAT网关弹性网口和私有实例弹性网口的日志组.运行查询以将目标地址设置 为“like 198.51.100.2"并将源地址设置为“like 203.0”进行过滤.运行stats命令过滤源地址和目的地址传输的字节总和
4. 打开Amazon CloudWatch控制台.选择包含NAT网关弹性网口和私有实例弹性网口的日志组.运行査询以将目标地 址设置为“like 198.51.100.2"并将源地址设置为“like 203.0"进行过滤.运行stats命令过滤源地址和目的地址传输的字节总 和

答案:D

解析： 问题已经指出从Internet入站到私有IP有一个Action=Accept.目标是确定这是请求流量还是未经请求的流量.如果请 求，流量最初会从私有IP地址发起，然后接收返回流量.如果未经请求，则不会有从私有IP地址出站的初始流量.

Q128 -家公司有一个对公司业务至关重要的遗留单一应用程序.该公司在运行Amazon Linux 2的Amazon EC2实例 上托管应用程序.该公司的应用程序团队收到法律部门的指示，要求将实例的加密Amazon Elastic Block Store (Amazon EBS)卷中的数据备份到Amazon S3存储桶.应用程序团队没有实例的管理SSH密钥对.应用程序必须继续为用户服 务.

哪种解决方案可以满足这些要求？

1. 将角色附加到具有写入Amazon S3权限的实例.使用AWS Systems Manager会话管理器选项获取对实例的访问权 限并运行命令以将数据复制到Amazon S3
2. 创建实例的映像并打开重启选项.从映像启动一个新的EC2实例.将具有写入Amazon S3权限的角色附加到新实例. 运行命令将数据复制到Amazon S3
3. 使用 Amazon Data Lifecycle Manager (Amazon DLM)拍摄 EBS 卷的快照.将数据复制到 Amazon S3
4. 创建实例的图像.从映像启动一个新的EC2实例.将具有写入Amazon S3权限的角色附加到新实例.运行命令将数据 复制到Amazon S3

答案:A

解析：

Q129.一家公司在单个Amazon EC2实例上托管一个关键应用程序.该应用程序使用Amazon ElastiCache for Redis单 节点集群作为内存数据存储该应用程序使用Amazon RDS for MariaDB数据库实例作为关系数据库.为了使应用程序正 常运行，基础设施的每一部分都必须健康并且必须处于活动状态.

解决方案架构师需要改进应用程序的体系结构，以便基础架构可以自动从故障中恢复，停机时间尽可能短.

哪些步骤组合可以满足这些要求？(选择三个.)

1. 使用Elastic Load Balancer在多个EC2实例之间分配流量.确保EC2实例是具有至少两个实例容量的Auto Scaling组的一部分
2. 使用弹性负载均衡器在多个EC2实例之间分配流量.确保EC2实例配置为无限制模式
3. 修改数据库实例以在同一可用区中创建只读副本.在故障场景中将只读副本提升为主数据库实例
4. 修改数据库实例以创建跨两个可用区的Multi\_AZ部署
5. 为ElastiCache for Redis集群创建一个复制组.将集群配置为使用至少具有两个实例容最的Auto Scaling组
6. 为ElastiCache for Redis集群创建一个复制组.在集群上启用多可用区

答案:ADF

解析：

Q130.-家公司的环境只有一个AWS账户.解决方案架构师正在审查环境以推荐公司可以改进的地方，特别是在访问 AWS管理控制台方面.公司的IT支持人员目前访问控制台以执行管理任务，向已映射到他们的指定IAM用户进行身份 验证职业角色.

IT支持人员不想再同时维护他们的Active Directory和IAM用户帐户.他们希望能够使用现有的Active Directory凭据 访问控制台.解决方案架构师使用AWS IAM Identity Center (AWS Single Sign-On)来实现此功能.

哪种解决方案能够最经济有效地满足这些要求？

1. 在 AWS Organizations 中创建•个组织.在 Organizations 中开启 IAM Identity Center 功能.

在 AWS Directory Service 中为 Microsoft Active Directory (AWS Managed Microsoft AD)创建和配置目录，并双向信任 公司的本地Active Directory.配置IAM Identity Center并将AWS Managed Microsoft AD目录设置为身份源.创建权限 集并将它们映射到AWS Managed Microsoft AD目录中的现有组

1. 在 AWS Organizations 中创建一个组织.在 Organizations 中打开 IAM Identity Center 功能.

创建和配置AD连接器以连接到公司的本地Active Directory.

配置IAM身份中心并选择AD连接器作为身份源.创建权限集并将它们映射到公司Active Directory中的现有组

1. 在AWS Organizations中创建•个组织.为该组织启用所有功能.在AWS Directory Service中爲Microsoft Active Directory (AWS Managed Microsoft AD)创建和配置目录，并双向信任公司的本地 Active Directory.配置 IAM Identity Center并选择AWS Managed Microsoft AD目录作为身份源.

创建权限集并将它们映射到AWS Managed Microsoft AD目录中的现有组

1. 在AWS Organizations中创建•个组织.打开组织的所有功能.创建和配置AD Connector以连接到公司的本地 Active Directory配置IAM Identity Center并将AD Connector设置为身份源.创建权限集并将它们映射到公司Active Directory中的现有组.

答案:B

*解析:*

Q131.—家公司正在使用本地Active Directory服务进行用户身份验证.该公司希望使用相同的身份验证服务登录公司使 用AWS Organizations的AWS賑户.本地环境和公司的所有AWS账户之间己经存在AWS站点到站点VPN连接. 公司的安全策略要求根据用户组和角色对帐户进行有条件的访问.用户身份必须在一个位置进行管理.

哪种解决方案可以满足这些要求？

1. 配置 AWS IAM Identity Center (AWS Single Sign-On)以使用 SAML2.0 连接到 Active Directory,使用跨域身份管理 系统(SCIM)v2.0协议启用自动配置.使用基于属性的访问控制(ABAC)授予对AWS帐户的访问权限
2. 使用IAM身份中心作为身份源配置AWS IAM身份中心(AWS单点登录).使用跨域身份管理系统(SCIM)v2.0协 议启用自动配置.使用IAM Identity Center权限集授予对AWS账户的访问权限
3. 在公司的 个AWS账户中，配置AWS Identity and Access Management (IAM)以使用SAML 2.0身份提供商.供 应映射到联合身份用户的IAM用户.授予与Active Directory中相应组对应的访问权限.使用跨账户IAM用户授予对所 需AWS账户的访问权限
4. 在公司的 个 AWS 账户中，配置 AWS Identity and Access Management (IAM)以使用 OpenlD Connect (OIDC) 身份提供商.为与Active Directory中的适当组对应的联合用户提供访问AWS账户的权限的IAM角色.使用跨账户 IAM授予对所需AWS账户的访问权限

角色

答案:B

解析：

Q132.一家公司正在通过基于REST的API向多个客户提供天气数据.该API由Amazon API Gateway托管，并为每个 API操作集成了不同的AWS Lambda函数.该公司使用Amazon Route 53进行DNS,并创建了 weather.example.com的 资源记录.该公司将API的数据存储在Amazon DynamoDB表中.该公司需要一种解决方案，使API能够故障转移到不 同的AWS区域.

哪种解决方案可以满足这些要求？

1. 在新区域中部署•组新的Lambda函数.更新API网关API以使用边缘优化的API端点，并将来自两个区域的 Lambda函数作为目标将DynamoDB表转换为全局表：
2. 在另一个区域部署新的API网关API和Lambda函数.将Route 53 DNS记录更改为多值答案.将两个API网关 API添加到答案中.启用目标健康监控.将DynamoDB表转换为全局表
3. 在另•个区域部署新的API网关API和Lambda函数.将Route 53 DNS记录更改为故障转移记录.启用目标健康 监控.将DynamoDB表转换为全局表
4. 在新区域部署新的API网关API.将Lambda函数更改为全局函数.

将Route 53 DNS记录更改为多值答案.将两个API网关API添加到答案中.

启用目标健康监控.将DynamoDB表转换为全局表

答案:C

解析：

Q133.公司的工厂和自动化应用程序在单个VPC中运行.超过20个应用程序在Amazon EC2> Amazon Elastic Container Service (Amazon ECS)和 Amazon RDS 的组合上运行

该公司的软件工程师分布在三个团队中.三个团队之一拥有每个应用程序，每个团队负责其所有应用程序的成本和性能.团 队资源具有代表其应用程序和团队的标签.团队使用IAM访问权限进行日常活动.

公司需要确定每月AWs账单上的哪些成本归因于每个应用程序或团队.公司还必须能够创建报告来比较过去12个月的 成本并帮助预测未来12个月的成本.解决方案架构师必须推荐提供这些成本报告的AWs计费和成本管理解决方案.

哪种行动组合将满足这些要求？(选择三项.

1. 激活代表应用程序和团队的用户定义的成本分配标签
2. 激活代表应用程序和团队的AWS生成的成本分配标签
3. 为Billing and Cost Management中的每个应用程序创建一个成本类别
4. 激活 IAM 对 Billing and Cost Management 的访问
5. 制定成本预算
6. 启用 Cost Explorer

答案:ADF

解析：

Q134.•家零售公司在AWS上运行其电子商务应用程序.该应用程序在应用程序负载均衡器（ALB）后面的Amazon EC2实例上运行.该公司使用Amazon RDS数据库实例作为数据库后端.Amazon CloudFront配*置C ~*个指向ALB的 源.缓存静态内容.Amazon Route 53用于托管所冇公共区域.

更新应用程序后，ALB有时会返回502状态代码（错误网关）错误.根本原因是返回给ALB的格式错误的HTTP标头. 当解决方案架构师在错误发生后立即重新加载网页时，网页成功返冋.

在公司处理该问题时，解决方案架构师需要向访问者提供自定义错误页面，而不是标准的ALB错误页面.

哪种步骤组合能够以最少的操作开销满足此要求？（选择两个.）

1. 创建一个Amazon S3存储桶.配置S3存储桶以托管静态网页.将自定义错误页面上传到Amazon S3
2. 如果ALB健康检査响应Target.FailedHealthChecks大于0,则创建Amazon CloudWatch警报以调用AWS Lambda函数.配置Lambda函数以修改ALB上的转发规则以指向可公开访问的Web服务器
3. 通过添加健康检查修改现有的Amazon Route 53记录.如果健康检査失败，则配置回退目标.修改DNS记录以指向 可公开访问的网页
4. 如果ALB健康检査响应Elb.lntemalError大于0,则创建Amazon CloudWatch警报以调用AWS Lambda函数. 配置Lambda函数以修改ALB的转发规则以指向公共可访问的Web服务器.
5. 通过配置CloudFront自定义错误页面添加自定义错误响应.修改DNS记录以指向可公开访问的网页

答案:AE

解析：

Q135.某公司注册了 10个新域名.该公司使用这些域进行在线营销.该公司需要一种解决方案，将在线访问者重定向到每个 域的特定URL.所有域和目标URL都在JSON文档中定义.所有DNS记录均由Amazon Route 53管理.

解决方案架构师必须实施接受HTTP和HTTPS请求的武定向服务.

解决方案架构师应该采取哪些步骤组合来以最少的操作工作量来满足这些要求？（选择三个

1. 创建一个在Amazon EC2实例上运行的动态网页.配置网页以结合使用JSON文档和事件消息来査找和响应重定向 URL
2. 创建-个包含HTTP和HTTPS侦听器的应用程序负载均衡嚣
3. 创建•个AWS Lambda函数，该函数结合使用JSON文档和事件消息来査找和响应重定向URL
4. 使用具有自定义域的Amazon API Gateway API发布AWS Lambda函数
5. 创建•个 Amazon CloudFront 分配.部署 Lambda@Edge 函数
6. 使用AWS Certificate Manager （ACM）创建SSL证书.包括域作为主题备用名称.

答案:BCE

*解析:*

Q136.一家公司有一个在本地环境中运行的物联网平台.该平台由一个使用MQTT协议连接到物联网设备的服务器组成. 该平台至少每5分钟从设备收集一次遥测数据.该平台还将设备元数据存储在MongoDB集群中.

安装在本地计算机上的应用程序运行定期作业来聚合和转换遥测和设备元数据.该应用程序创建用户使用在同一本地计算 机上运行的另一个Web应用程序査看的报告.定期作业需要120-600秒才能运行但是，Web应用程序始终在运行.

该公司正在将该平台迁移到AWS,并且必须减少堆栈的运营开销.

哪些步骤组合将以最少的操作开销满足这些要求？（选择三个.）

1. 使用AWS Lambda函数连接到物联网设备
2. 配置物联网设备发布到AWS物联网核心
3. 将元数据写入Amazon EC2实例上的自我管理的MongoDB数据库
4. 将元数据写入 Amazon DocumentDB （兼容 MongoDB）
5. 使用AWS Step Functions状态机和AWS Lambda任务来准备报告并将报告写入Amazon S3.使用具有S3来源 的Amazon CloudFront来提供报告
6. 使用带有 Amazon EC2 实例的 Amazon Elastic Kubemetes Service （Amazon EKS）集群来准备报告.使用 EKS 集 群中的入口控制器来提供报告 答案:BDE

Q137 -家公司正在AWS云中设计其网络配置.该公司使用AWS Organizations来管理多账户设置.公司有3个0U,每 个0U包含100多个AWS账户.每个账户都有一个VPC,每个0U中的所有VPC都在同一个AWS区域中.

所有AWS账户的CIDR范围不重叠.公司需要卖现同一个0U内的VPC可以互通，但不能与其他0U内的VPC互通 的解决方案

哪种解决方案能够以最少的运营开销满足这些要求？

1. 创建一个AWS CloudFormation堆栈集，在每个0U中的账户之间建立VPC对等.

在每个OU中配置堆栈集

1. 在每个0U中，创建一个具有单个VPC的专用网络帐户.使用AWS Resource Access Manager (AWS RAM)与

OU中的所有其他账户共享此VPC.在网络帐户和0U中的每个帐户之间创建VPC对等连接

1. 在每个OU的账尸中配置一个中转网关.使用AWS Resource Access Manager (AWS RAM)在整个组织中共享中转 网关.为每个VPC创建中转网关VPC连接
2. 在每个OU中，创建一个具有单个VPC的专用网络帐户.在网络帐户和0U中的其他帐户之间建立VPN连接.使 用第三方路由软件在VPC之间路由可传递流量

答案:C

解析:

Q138l家公司正在运行一个使用Amazon ElastiCache for Redis集群作为缓存层的应用程序.最近的安全审计显示该公 司已为ElastiCache配置了静态加密.但是，该公司并未将ElastiCache配置为在传输过程中使用加密.此外，用户无需 身份验证即可访问缓存.

解决方案架构师必须进行更改以要求用户身份验证并确保公司使用端到端加密.

哪种解决方案可以满足这些要求？

1. 创建一个AUTH令牌.将令牌作为加密参数存储在AWS System Manager Parameter Store中.使用AUTH创建一 个新集群，并配置传输中加密.更新应用程序以在必要时从Parameter Store检索AUTH令牌并使用AUTH令牌进行身 份验证
2. 创建一个AUTH令牌.将令牌存储在AWS Secrets Manager中.配置现有集群以使用AUTH令牌，并配置传输中加 密.更新应用程序以在必要时从Secrets Manager检索AUTH令牌并使用AUTH令牌进行身份验证
3. 创建SSL证书.将证书存储在AWS Secrets Manager中.创建一个新集群，并配置传输中加密.更新应用程序以在必 要时从Secrets Manager检索SSL证书并使用该证书进行身份验证
4. 创建SSL证书.将证书存储在AWS Systems Manager Parameter Store中，作为加密的高级参数.更新现有集群以 配置传输中加密.更新应用程序以在必要时从Parameter Store检索SSL证书并使用该证书进行身份验证

答案:B

解析：

Q139.-家公司运营着•个客户服务中心，该中心接听电话并通过短信自动向所有客户发送•份受管理的、交互式的、双 向的体验调査.支持客户服务中心的应用程序在公司托管在本地数据中心的机器上运行.公司使用的硬件老III,公司正在经 历系统停机.公司希望将系统迁移到AWS以提高可靠性・

哪种解决方案能够以最少的持续运营开销满足这些要求？

1. 使用Amazon Connect替换旧的呼叫中心硬件.使用Amazon Pinpoint向客户发送短信调查
2. 使用 Amazon Connect 替换旧的呼叫中心硬件.使用 Amazon Simple Notification Service (Amazon SNS)向客户发 送短信调查
3. 将呼叫中心软件迁移到Auto Scaling组中的Amazon EC2实例.使用EC2实例向客户发送短信调查
4. 使用Amazon Pinpoint替换旧的呼叫中心硬件并向客户发送短信调查

答案:A

Q140.一家零售公司在AWS上运行其电子商务应用程序.该应用程序在应用程序负载均衡器(ALB)后面的Amazon

EC2实例上运行.该公司使用Amazon RDS数据库实例作为数据库后端.Amazon CloudFront配置有一个指向ALB的 源.缓存静态内容.Amazon Route 53用于托管所有公共区域.

更新应用程序后，ALB有时会返回502状态代码(错误网关)错误.根本原因是返回给ALB的格式错误的HTTP标头. 当解决方案架构师在错误发生后立即重新加载网页时，网页成功返回.

在公司处理该问题时，解决方案架构师需要向访问者提供自定义错误页面，而不是标准的ALB借误页面.

哪种步骤组合能够以最少的操作开销满足此要求？(选择两个.)

1. 创建一个Amazon S3存储桶.配置S3存储桶以托管静态网页.将自定义错误页面上传到Amazon S3
2. 如果ALB健康检查响应Target.FailedHealthChecks大于O配置Lambda函数以修改ALB的转发规则以指向 可公开访问的Web服务器，则创建Amazon CloudWatch警报以调用AWS Lambda函数.
3. 通过添加健康检査修改现有的Amazon Route 53记录.如果健康检査失败，则配置回退目标.修改DNS记录以指向 可公开访问的网页
4. 如果ALB健康检査响应Elb.lntemalError大于O,则创建Amazon CloudWatch警报以调用AWS Lambda函数. 配置Lambda函数以修改ALB的转发规则以指向公共可访问的Web服务器
5. 通过配置CloudFront自定义错误页面添加自定义错误响应.修改DNS记录以指向可公开访问的网页

答案:AE

解析：

Q141.一家公司正在AWS云中运行应用程序.最近的应用程序指标显示响应时间不一致并且错误率显着增加对第三方 服务的调用导致了延迟.目前，应用程序通过直接调用AWS Lambda函数来同步调用第.三方服务.

解决方案架构师需要解耦第三方服务调用并确保所有调用最终完成.

哪种解决方案可以满足这些要求？

1. 使用 Amazon Simple Queue Service (Amazon SQS)队列来存储事件并调用 Lambda 函数
2. 使用AWS Step Functions状态机将事件传递给Lambda函数
3. 使用Amazon EventBridge规则将事件传递给Lambda函数，
4. 使用 Amazon Simple Notification Service (Amazon SNS)主题存储事件并调用 Lambda 函数

答案:A

解析:

Q142.一家公司在面向互联网的应用程序负载均衡器(ALB)后面的私有子网中的一组Amazon EC2实例上运行应用程 序.ALB是Amazon CloudFront分发的来源.包含各种AWS托管规则的AWSWAF WebACL与CloudFront分配关 联.

公司需要一种解决方案来防止互联网流量直接访问ALB.哪种解决方案能够以最少的运营开销满足这些要求？

1. 创建一个新的WebACL,其中包含与现有WebACL相同的规则.将新的WebACL与ALB相关联
2. 将现有的WebACL与ALB相关联
3. 向ALB添加安全组规则以仅允许来自AWS托管前綴列表的流量:用于CloudFront
4. 向ALB添加安全组规则以仅允许冬种CloudFront IP地址范围

答案:B

*解析:*

Q143.一家公司在AWS云中运行•个物联网应用程序.该公司拥有数百万个传感器，这些传感器从美国的房屋收集数据. 传感器使用MQTT协议连接并将数据发送到自定义MQTT代理・MQTT代理将数据存储在单个Amazon EC2实例上, 传感器通过名为iot.example.com的域连接到代理.该公司使用Amazon Route 53作为其DNS服务.该公司将数据存 储在 Amazon DynamoDB 中.

有几次，数据量使MQTT代理超载，导致传感器数据丢失.公司必须提高解决方案的可靠性.

哪种解决方案可以满足这些要求？

1. *为* MQTT 代理创建\_个 Application Load Balancer (ALB)和•个 Auto Scaling 组.使用 Auto Scaling 组作为 ALB 的日标.将Route 53中的DNS记录更新为别名记录.

将别名记录指向ALB.使用MQTT代理存储数据

1. 设置AWS loTCore以接收传感器数据.创建和配置自定义域以连接到AWS loT Core.更新Route 53中的DNS记 录以指向 AWS loT Core Data-ATS 端点.

配置AWS loT规则来存储数据

1. 创建网络负载平衡器(NLB).将MQTT代理设置为目标.创建-个AWS Global Accelerator加速器.将NLB设置为 加速器的端点.将Route 53中的DNS记录更新为多值应答记录.将Global Accelerator IP地址设置为值.使用MQTT 代理存储数据
2. 设置AWS loT Greengrass以接收传感器数据.更新Route 53中的DNS记录以指向AWS loT Greengrass终端 节点.配置AWS loT规则以调用AWS Lambda函数来存储数据

答案:B

解析：

Q144.解决方案架构师计划将关键的Microsoft SQL Server数据库迁移到AWS.由于数据库是遗留系统，解决方案架构 师会将数据库迁移到现代数据架构.解决方案架构师必须在停机时间接近零的情况下迁移数据库.

哪种解决方案可以满足这些要求？

1. 使用 AWS Application Migration Service 和 AWS Schema Conversion Tool (AWS SCT).^E迁移之前执行就地升级.

割接后将迁移后南数据导出到Amazon Aurora Serverless.将应用程序重新指向Amazon Aurora

1. 使用 AWS Databnse Migration Service (AWS DMS)重新托管数据库.将 Amazon S3 设置为目标.

设置变更数据捕获(CDC)复制当源和目标完全同步时，将数据从Amazon S3加载到Amazon RDS for Microsoft SQL Server数据库实例

1. 使用本机数据库髙可用性工具.将源系统连接到Amazon RDS for Microsoft SQL Server数据库实例.相应地配置复制. 数据复制完成后，将工作负载转移到Amazon RDS for Microsoft SQL Server数据库实例
2. 使用AWS应用程序迁移服务.在Amazon EC2上重新托管数据库服务器.数据复制完成后，分离数据库并将数据库 移动到Amazon RDS for Microsoft SQL Server数据库实例.重新附加数据库，然后切断所有网络

答案:B

解析：

Q145.-家公司在Amazon EC2实例上运行传统的Web应用程序.公司需要将应用程序重构为在容器上运行的微服务. 应用程序的不同版本存在于两个不同的环境中：生产和测试.应用程序的负载是可变的，但最小负载和最大负载是已知的. 解决方案架构师需要使用无服务器架构设计更新的应用程序，以最大限度地降低操作复杂性.

哪种解决方案能够最经济有效地满足这些要求？

1. 将容器镜像作为函数上传到AWS Lambda.为关联的Lambda函数配置并发限制以处理预期的峰值负载.在Amazon API Gateway中配置两个单独的Lambda集成：一个用于生产，一个用于测试
2. 将容器镜像上传到Amazon Elastic Container Registry (Amazon ECR).^用Fargate启动类型配置两个自动扩展的 Amazon Elastic Container Service (Amazon ECS)集群以处理预期负载.从ECR映像部署任务.配置两个单独的 Application Load Balancer以将流量定向到ECS集群
3. 将容器镜像上传到Amazon Elastic Container Registry (Amazon ECR).使用Fargate启动类型配置两个自动扩展的 Amazon Elastic Kubernetes Service (Amazon EKS)集群以处理预期负载.从ECR映像部署任务.配置两个单独的 Application Load Balancer以将流量定向到EKS食群
4. 将容器镜像上传到AWS Elastic Beanstalk.在Elastic Beanstalk中，为生产和测试创建单独的环境和部署配置两个 单独的应用程序负载均衡器以将流量定向到Elastic Beanstalk部署

答案:B

解析：

Q146.•家公司的交互式Web应用程序使用Amazon CloudFront分配来提供来自Amazon S3存储桶的图像.有时， 第三方工具会将损坏的图像提取到S3存储桶中.这种图像损坏会导致以后应用程序的用户体验不佳.该公司已成功实施 和测试Python逻辑来检测损坏的图像.

解决方案架构师必须推荐一种解决方案，以在摄取和服务之间以最小的延迟集成检测逻辑.

哪种解决方案可以满足这些要求？

1. 使用由查看者响应事件调用的Lambda@Edge函数
2. 使用由原始响应事件调用的Lambda@Edge函数
3. 使用调用AWS Lambda函数的S3事件通知
4. 使用调用AWS Step Functions状态机的S3事件通知

答案:B

解析：

Q147.解决方案架构师需要将数据从AWS账户中的Amazon S3存储桶复制到新AWS账户中的新S3存储桶.解决 方案架构师必须实施使用AWS CLI的解决方案.

哪种步骤组合可以成功复制数据？(选择三项)

1. 创建桶策略以允许源桶列出其内容并在目标桶中放置对象和设置对象ACL.将存储桶策略附加到目标存储桶
2. 创建存储桶策略以允许目标账户中的用户列出源存储桶的内容并读取源存储桶的对象.将存储桶策略附加到源存储桶
3. 在源账户中创建一个IAM策略.配置策略允许源账户的用户在源桶中列出内容和获取对象，在目标桶中列出内容、放 置对象和设置对象ACL.将策略附加到用户.
4. 在目标账户中创建IAM策略.配置策略允许目的账户的用户在源桶中列出内容和获取对象，在目的桶中列出内容、放 置对象和设置对象ACL.将策略附加到用户
5. 以源账户中的用户身份运行aws s3 sync命令.指定复制数据的源捅和目标桶
6. 以目标胀户中的用户身份运行awss3sync命令.指定复制数据的源桶和日标桶

答案：BDF

解析：

Q148.-家公司希望在AWS Organizations中跨公司组织内的开发人员账户优化AWS数据传输成本和计算成本.开发 人员可以在单个AWS区域配置VPC并启动Amazon EC2实例.EC2实例每天从Amazon S3检索大约1 TB的数 据.

开发人员活动导致EC2实例和S3存储桶之间的月度数据传输费用和NAT网关处理费用过高，以及高昂的计算成本. 该公司希望为开发人员在AWS账户中部署的任何EC2实例和VPC基础设施主动实施批准的架构模式.公司不希望这 种强制措施对开发人员执行任务的速度产生负面影响.哪种解决方案能够最经济有效地满足这些要求？

1. 创建SCP以防止开发人员启动未经批准的EC2实例类型.为开发人员提供AWS CloudFormation模板，以部署具 有S3接口端点的经批准的VPC配置.限定开发人员的IAM权限，以便开发人员只能使用CloudFormation启动 VPC资源
2. 使用AWS预算创建每日预测预算，以监控跨开发人员账户的EC2计算成本和S3数据传输成本.当预测成本是实 际预算成本的75%时，向开发团队发送警报.如果实际预算成本是100%.创建预算操作以终止开发人员的EC2实例和 VPC基础设施
3. 创建一个AWS Service Catalog产品组合，用户可以使用它来创建具有S3网关端点和批准的EC2实例的批准 VPC配置.与开发者帐户共享投资组合.配置AWs Service Catalog启动约束以使用已批准的IAM角色.限定开发人员的 IAM权限以仅允许访问AWS Service Catalog
4. 创建和部署AWS Config规则以监控开发人员AWS账户中EC2和VPC资源的合规性.如果开发人员启动未经批 准的EC2实例，或者如果开发人员创建没有S3网关端点的VPC.执行补救措施以终止未批准的资源

答案:C

解析：

Q149.一家公司最近收购了其他几家公司.每家公司都有一个单独的AWS账户，使用不同的计费和报告方法.收购公司已 将所有账户整合到AWS Organizations中的一个组织中.然而，收购公司发现很难生成包含对所有团队有意义的组的成本 报告.收购公司的财务团队需要一个解决方案来通过自我管理的应用程序报告所有公司的成本.

哪种解决方案可以满足这些要求？

1. 为组织创建•份AWS成本和使用报告.在报告中定义标签和成本类别.在Amazon Athena中创建•个表.基于 Athena表创建Amazon QuickSight数据集.与财务团队共享数据集
2. 为组织创建AWS成本和使用情况报告.在报告中定义标签和成本类别.在AWS Cost Explorer中创建专用模板，财务 部门将使用该模板构建报告
3. 创建•个Amazon QuickSight数据集，用于从AWS价目表查询API接收支出信息.与财务团队共享数据集
4. 使用AWS价目表查询API收集账户消费信息，在AWS Cost Explorer中创建专用模板，财务部门将使用该模板构 建报告

答案:A

解析:

Q150-家公司希望使用AWS创建业务连续性解决方案，以防公司的主要本地应用程序岀现故障.该应用程序在同时运 行其他应用程序的物理服务器上运行.公司计划迁移的本地应用程序使用MySQL数据库作为数据存储.公司的所有本地 应用程序都使用与Amazon EC2兼容的操作系统.哪种解决方案将以最少的运营开销实现公司的目标？

1. 在源服务器上安装AWS Replication Agent.包括MySQL服务器.为所有服务器设置复制.为定期演练启动测试实例. 在发生故障事件时切换到测试实例以故障转移工作负载
2. 在源服务器上安装AWS Replication Agent.包括MySQL服务器.在目标AWS区域中初始化AWS Elastic Disaster Recovery.定义启动设置.从最近的时间点开始频繁执行故障转移和故障回复
3. 创建 AWS Database Migration Service (AWS DMS)复制服务器和一个目标 Amazon Aurora MySQL 数据库集群来 托管数据库.创建DMS复制任务，将现有数据复制到目标数据库集群.创建本地AWS Schema Conversion Tool (AWS SCT)更改数据捕获(CDC)任务以保持数据同步.从兼容的基本AMI开始，在EC2实例上安装其余软件
4. 在本地部署AWS Storage Gateway Volume Gateway.在所有本地服务器上装载卷在新卷上安装应用程序和MySQL 数据库.定期拍摄快照.

从兼容的基本AMI开始，在EC2实例上安装所有软件.在EC2实例上启动卷网关.从最新的快照恢复卷.在发生故障事 件时在EC2实例上安装新卷

答案:C

解析:

Q151.-家公司在Amazon S3中将新应用程序作为静态网站运行.该公司己将应用程序部署到生产AWS账户并使用 Amazon Cloud Front交付网站.该网站调用Amazon API Gateway REST API. AWS Lambda函数支持每个API方法.该 公司希望每2周创建•份CSV报告，以显示每个API Lambda函数的建议配置内存、建议成本以及当前配置与建议 之间的价格差异.公司会将报告存储在S3存储桶中.哪种解决方案能够以最短的开发时间满足这些要求？

1. 创建一个Lambda函数，从Amazon CloudWatch Logs中提取每个API Lambda函数的指标数据，持续2周.将 数据整理成表格格式.将数据作为.csv文件存储在S3存储桶中.创建Amazon EventBridge规则以安排Lambda函 数每2周运行一次
2. 选择加入 AWS Compute Optimizer.创建调用 ExportLambdaFunctionRecommendations 操作的 Lambda 函数. 将.csv文件导岀到S3存儲桶创建Amazon EventBridge规则以安排Lambda函数每2周运行一次
3. 选择加入AWS Compute Optimizer.设置增强的基础架构指标.在Compute Optimizer控制台中，安排一个作业将 Lambda建议导出到一个.csv文件.每2周将文件存储在S3存储桶中
4. 为生产账户购买AWS业务支持计划.选择加入AWS Compute Optimizer for AWS Trusted Advisor检査.在Trusted Advisor控制台中.安排作业将成本优化检查导出到a.csv文件.每2周将文件存储在S3存储桶中

答案:B

解析:

Q152,解决方案架构师正在重新设计公司在本地托管的三层应用程序.该应用程序根据用户配置文件提供个性化推荐.该公 司己经有一个AWS账户，并配置了一个VPC来托管应用程序.前端是在本地VM中运行的基于Java的应用程序.该 公司在物理应用服务器上托管个性化模型，并使用TensorFlow来实现该模型.个性化模型使用人工智能和机器学习 (AI/ML).公司将用户信息存储在Microsoft SQL Server数据库中.Web应用程序调用个性化模型，该模型从数据库中读 取用户配置文件并提供建议..该公司希望将重新设计的应用程序迁移到AWS.哪种解决方案能够以最少的运营开销满足此 要求？

1. 使用AWS Server Migration Service (AWS SMS)将本地物理应用程序服务•器和Web应用程序虚拟机迁移到AWS. 使用 AWS Database Migration Service (AWS DMS)将 SQL Server 数据库迁移到 Amazon RDS for SQL Server
2. 导出个性化模型.将模型工件存储在Amazon S3中.将模型部署到Amazon SageMaker并创建•个端点在AWS Elastic Beanstalk 中托管 Java 应用程序.使用 AWS Database Migration Service (AWS DMS)将 SQLServer 数据库 迁移到 Amazon RDS for SQL Serve
3. 使用AWS Application Migration Service将本地个性化模型和VM迁移到Auto Scaling组中的Amazon EC2实 例.使用 AWS Database Migration Service (AWS DMS)将 SQL Server 数据库迁移到 EC2 实例
4. 将个性化模型和Java应用程序容器化.使用Amazon Elastic Kubernetes Service (Amazon EKS)托管节点组将模 型和应用程序部署到Amazon EKS.

在 VPC 中托管节点组.使用 AWS Database Migration Service (AWS DMS)将 SQL Server 数据库迁移到 Amazon RDS for SQL Server

答案:A

解析：

Q153l家公司计划将1000台本地服务器迁移到AWS.服务器在公司数据中心的多个VMware集群上运行作为迁移 计划的•部分，公司希望收集服务指标，例如CPU详细信息、RAM使用操作系统信息和正在运行的进程.然后公司想 查询和分析数据.

哪种解决方案可以满足这些要求？

1. 在本地主机上部署和配置AWS Agentless Discovery Connector虚拟设备.在AWS Migration Hub中配置数据探索. 使用AWS Glue对数据执行ETL作业.使用Amazon S3 Select査询数据
2. 仅从本地主机导出VM性能信息.直接将所需数据导入AWS Migration Hub.Sl新Migration Hub中任何缺失的信息. 使用Amazon QuickSight査询数据
3. 创建脚本以自动从本地主机收集服务器信息.使用AWS CLI运行put-resource-attributes命令以将详细的服务器数 据存储在 AWS Migration Hub 中.

直接在Migration Hub控制台查询数据

1. 将AWS Application Discovery Agent部署到每个本地服务器.在AWS Migration Hub中配置数据探索.使用 Amazon Athena对Amazon S3中的数据运行预定义查询

答案:D

解析：

Q154.一家公司最近使用重新平台化策略完成了从本地数据中心到AWS云的迁移.其中一台迁移的服务器正在运行一个 关键应用程序所依赖的遗留简单邮件传输协议(SMTP)服务.

该应用程序向公司的客户发送出站电子邮件消息.旧版SMTP服务器不支持TLS加密并使用TCP端口 25.应用程序 只能使用SMTP.公司决定使用Amazon Simple Email Service (Amazon SES)并停用旧的SMTP服务器.公司己创建 并验证SES域.公司己解除SES限制.

公司应如何修改应用程序以从Amazon SES发送电子邮件？

TLS Wrapper 连接到 Amazon SES.创建一个具有 ses:SendEmail 和 ses:SendRawEmail 权 角色附加到Amazon EC2实例

1. 配置应用程序以使用

限的IAM角色.将IAM

1. 配置应用程序以使用

SES进行身份验证

1. 配置应用程序以使用

STARTTLS连接到Amazon SES.获取Amazon SES SMTP凭证.使用凭据通过Amazon

SES API发送电子邮件消息.创建•个具有ses:SendEmail和ses:SendRawEmail权限的

IAM角色.使用IAM角色作为Amazon SES的服务角色

1. 配置应用程序以使用AWS SDK发送电子邮件.为Amazon SES创建一个IAM用户.生成API访问密钥.使用访问 密钥向Amazon SES进行身份验证

答案:C

解析：

Q155.一家公司正在更新客户用来在线下订单的应用程序.最近，不良行为者对应用程序的攻击次数有所増加.

该公司将在Amazon Elastic Container Service (Amazon ECS)集群上托管更新后的应用程序.该公司将使用Amazon DynamoDB来存储应用程序数据.公共应用程序负载均衡器(ALB)将为最终用户提供对应用程序的访问权限.公司必须 防止攻击并确保业务连续性，同时在持续攻击期间将服务中断降至最低.哪种步骤组合可以最经济高效地满足这些要求？

(选择两个.)

1. 创建一个以ALB作为源的Amazon CloudFront分配.在CloudFront域上添加自定义标头和随机值.如果标头和值 匹配，则将ALB配置为有条件地转发流量
2. 在两个AWS区域部署应用程序.配置Amazon Route 53以同等权重路由到两个区域
3. 为Amazon ECS任务配置自动缩放.创建DynamoDB加速器(DAX)集群
4. 配置 Amazon ElastiCache 以减少 DynamoDB 的开销
5. 部署包含适当规则组的AWS WAF WebACL.将 Web ACL与Amazon CloudFront分配相关联

答案:AE

解析：

Q156.一家公司在本地运行Intranet应用程序.公司想要配置应用程序的云备份.该公司为此解决方案选择了 AWS

Elastic Disaster Recovery.公司要求复制流星不通过公共互联网传输.该应用程序也不得可从Internet访问.公司不希望 此解决方案占用所有可用的网络带宽，因为其他应用程序需要带宽.哪种步骤组合可以满足这些要求？(选择三项.)

1. 创建-个至少有两个私有子网、两个NAT网关和-个虚拟私有网关的VPC
2. 创建-个至少有两个公共子网、一个虚拟专用网关和一个互联网网关的VPC
3. 在本地网络和目标AWS网络之间创建AWS Site-to-Site VPN连接
4. 在本地网络和目标AWS网络之间创建AWS Direct Connect连接和Direct Connect冋关
5. 在配置复制服务器期间，选择使用私有IP地址进行数据复制的选项
6. 在为目标服务器配置启动设置期间，选择确保恢复实例的私有IP地址与源服务器的私有IP地址相匹配的选项

答案:ADF

解析：

Q157.—家公司使用Amazon S3在各种存储类别中存儲文件和图像.公司的S3成本在过去一年中大幅增加. 解决方案架构师需要审查过去12个月的数据趋势并确定对象的适当存储类別.

哪种解决方案可以满足这些要求？

1. 下载过去12个月的S3使用情况的AWS成本和使用情况报告.查看AWS Trusted Advisor关于节省成本的建议
2. 使用S3存储类分析.将数据趋势导入Amazon QuickSight控制面板以分析存储趋势
3. 使用Amazon S3 Storage Lens.fl-级默认仪表板以包含存储趋势的高级指标
4. 使用S3访问分析器.下载过去12个月的Access Analyzer for S3报告.将.csv文件导入Amazon QuickSight控 制面板 答案:C

Q158.一家公司正在构建一个无服务器应用程序，该应用程序在附加到VPC的AWS Lambda函数上运行.该公司需要 将该应用程序与来自外部提供商的新服务集成.外部提供商仅支持来自允许列表中的公共IPv4地址的请求.在应用程序 可以开始使用新服务之前，公司必须向外部提供商提供一个公共IP地址.

哪种解决方案将使应用程序能够访问新服务？

1. 部署一个NAT网关.将弹性IP地址与NAT网关相关联.配置VPC使用NAT网关
2. 部署仅出口互联网网关.将弹性IP地址与仅出口互联网网关相关联.在Lambda函数上配置弹性网络接口以使用仅 出口互联网网关
3. 部署互联网网关.将弹性IP地址与互联网网关相关联.配置Lambda函数以使用互联网网关
4. 部署互联网网关.将弹性IP地址与互联网网关相关联.在公共VPC路由表中配置默认路由以使用互联网网关

答案:D

解析：

Q159.解决方案架构师希望在单个AWS账户中优化成本并适当调整Amazon EC2实例的大小.解决方案架构师希望确 保实例根据CPU、内存和网络指标进行优化

解决方案架构师应该采取哪些步骤组合来满足这些要求？（选择两个.）

1. 为账户购买 AWS Business Support 或 AWS Enterprise Support
2. 打开AWS Trusted Advisor并査看任何“低利用率Amazon EC2实例”建议
3. 安装Amazon CloudWatch代理并在EC2实例上配置内存指标收集
4. 在AWS账户中配置AWS Compute Optimizer以接收结果和优化建议
5. 为感兴趣的AWS区域、实例系列和操作系统创建EC2实例储蓄计划

答案:BC

解析：

Q160.一家公司允许用户从自定义应用程序上传图像.上传过程调用AWS Lambda函数处理图像并将其存储在Amazon S3存储桶中.应用程序通过使用特定函数版本ARN调用Lambda函数.Lambda函数通过使用环境变量接受图像处理 参数.公司经常调整Lambda函数的环境变量，以达到最佳的图像处理输出.该公司测试不同的参数，并在验证结果后发布 带有更新环境变量的新功能版本.此更新过程还需要频繁更改自定义应用程序以调用新功能版本ARN.这些更改会导致用 户中断.解决方案架构师需要简化此过程以最大程度地减少对用户的干扰期S种解决方案能够以最少的运营开销满足这些 要求？

1. 直接修改发布的Lambda函数版本的环境变量，使用SLATEST版本测试图片处理参数
2. 创建•个Amazon DynamoDB表来存储图像处理参数.修改Lambda函数以从DynamoDB表中检索图像处理参数
3. 直接在Lambda函数内编码图片处理参数，去掉环境变量.公司更新参数时发布新功能版本
4. 创建一个Lambda函数别名.修改客户端应用程序以使用函数別名ARN.当公司完成测试时，重新配置Lambda别名 以指向函数的新版本

答案:D

解析：

Q161.一家公司在AWSOrganizations中有一个组织，其中包括公司每个部门的单独AWS账户.来自不同部门的应用团 队独立开发和部署解决方案

该公司希望降低计算成本并适当地跨部门管理成本.公司还希望提高各个部门计费的可见性.公司不希望在选择计算资源 时失去运营灵活性.

哪种解决方案可以满足这些要求？

1. 为每个部门使用AWS预算.使用标签编辑器将标签应用于适当的资源.

购买EC2实例储蓄计划

1. 配置AWS Organizations以使用整合账单.实施标识部门的标记策略,使用SCP将标签应用于适当的资源.购买EC2 实例储蓄计划
2. 配置AWS Organizations以使用整合账单.实施标识部门的标记策略.使用标签编辑器将标签应用于适当的资源.购买 计算储蓄计划
3. 为每个部门使用AWS预算.使用SCP将标签应用于适当的资源.购买计算储蓄计划

答案:C

解析：

Q162.•家公司正在使用Amazon API Gateway和AWS Lambda开发新的无服务器API.该公司将Lambda函数与 API Gateway集成在一起，以使用多个共享库和自定义类.

解决方案架构师需要简化解决方案的部署并优化代码重用.

哪种解决方案可以满足这些要求？

1. 将共享库和自定义类部署到Docker映像中.将图像存储在S3存储桶中创建一个使用Docker图像作为源的 Lambda层.将API的Lambda函数部署为Zip包.配置包以使用Lambda层
2. 将共享库和自定义类部署到Docker映像.将图像上传到Amazon Elastic Container Registry (Amazon ECR).创建一 个使用Docker映像作为源的Lambda层.将API的Lambda函数部署为Zip包.配置包以使用Lambda层
3. 使用AWS Fargate启动类型将共享库和自定义类部署到Amazon Elastic Container Service (Amazon ECS)中的 Docker容器.将API的Lambda函数部署为Zip包.配置包以使用己部署的容器作为Lambda层
4. 将API的Lambda函数的共享库、自定义类和代码部署到Docker映像.将图像上传到Amazon Elastic Container Registry (Amazon ECR).配置API的Lambda函数以使用Docker映像作为部署包

答案:D

Q163.一家快递公司需要将其第三方路线规划应用程序迁移到AWS.第三方从公共注册表提供受支持的Docker映像.该 图像可以在生成路线图所需的任意数量的容器中运行.

该公司已将送货区域划分为带有供应中心的部分，以便送货司机从中心到客户的行进距离尽可能短.为了减少生成路线图 所需的时间，每个部分都使用自己的一组Docker容器，这些容器具有自定义配置，仅在该部分区域处理订单.

公司需要能够根据运行容器的数量经济高效地分配资源 哪种解决方案能够以最少的运营开销满足这些要求？

1. 在 Amazon EC2 上创建一个 Amazon Elastic Ku be metes Service (Amazon EKS)集群.使用 Amazon EKS CLI 通 过使用-tags选项将自定义标签分配给pod,在pod中启动规划应用程序
2. 在 AWS Fargate 上创建一个 Amazon Elastic Kubernetes Service (Amazon EKS)集群.使用 Amazon EKS CLI!启 动规划应用程序.使用AWS CLI标签资源API调用将自定义标签分配给容器
3. 在 Amazon EC2 ±创建一个 Amazon Elastic Container Service (Amazon ECS)集群.使用 run-tasks 设置为 true 的AWS CLI通过使用-tags选项将自定义标签分配给任务来启动规划应用程序
4. 在 AWS Fargate 上创建一个 Amazon Elastic Container Service (Amazon ECS)集群.使用 AWS CLI run-task 命令 并将enableECSManagedTags设置为true以启动规划应用程序.

使用-tags选项为任务分配自定义标签

答案:D

解析：

Q164, •家公司在AWS上运行•个应用程序，该公司从几个不同的来源整理数据,该公司使用专有算法来执行数据转换和 聚合.公司执行ETL流程后，将结果存储在Amazon Redshift表中.该公司将这些数据出售给其他公司.公司从Amazon Redshift表中以文件形式下载数据，并使用FTP将文件传输给多个数据客户.数据客户的数量显着增长.数据客户的管理 变得困难,该公司将使用AWS Data Exchange创建一个数据产品，该公司可以使用该产品与客户共享数据，该公司希望在 公司共享数据之前确认客户的身份.当公司发布数据时，客户还需要访问最新的数据.

哪种解决方案能够以最少的运营开销满足这些要求？

1. 使用适用于API的AWS Data Exchange与客户共享数据.配置订阅验证.在生产数据的公司的AWS账户中，创建一 个Amazon API Gateway数据API服务集成Amazon Redshift要求数据客户订阅数据产品
2. 在生产数据的公司的AWS账户中，通过将AWS Data Exchange连接到Redshift集群来创建一个AWS Data Exchange数据共享.配置订阅验证.要求数据客户订阅数据产品
3. 定期将数据从Amazon Redshift表下载到Amazon S3存储桶.使用AWS Data Exchange for S3与客户共享数据. 配置订阅验证.要求数据客户订阅数据产品
4. 将Amazon Redshift数据发布到AWS Data Exchange上的开放数据.要求客户订阅AWS Data Exchange中的数 据产品.在生成数据的公司的AWS账户中，将基于IAM资源的策略附加到Amazon Redshift表以仅允许访问经过验证 的AWS账户

答案:D

解析：

Q165.一家公司需要跨两个AWS区域监控越来越多的Amazon S3存储桶.该公司还需要跟踪在Amazon S3中加密的 对象的百分比.公司需要一个仪表板来为内部合规团队显示信息.哪种解决方案能够以最少的运营开销满足这些要求？

1. 在每个区域创建•个新的S3 Storage Lens控制面板来跟踪存储桶和加密指标将来自两个区域控制面板的数据聚合 到Amazon QuickSight中供合规团队使用的单个控制面板
2. 在每个区域部署•个AWS Lambda函数来列出桶的数量和对象的加密状态.将此数据存储在Amazon S3中.使用

Amazon Athena查询在Amazon QuickSight中的自定义控制面板上为合规团队显示数据

1. 使用S3 Storage Lens默认仪表板来跟踪存储桶和加密指标.授予合规团队直接在S3控制台中访问仪表板的权限
2. 创建•个Amazon EventBridge规则来检测AWS CloudTrail事件以创建S3对象.配置规则以调用AWS Lambda 函数以在Amazon DynamoDB中记录加密指标.使用Amazon QuickSight在控制面板中为合规团队显示指标

答案:C

解析：

Q166.一家公司正在使用Amazon OpenSearch Service分析数据.该公司将数据从使用S3标准存储的Amazon S3存 储桶加载到具有10个数据节点的OpenSearch服务集群中.数据在集群中驻留1个月以供读取.只有分析.1个月后， 公司从集群中删除包含数据的索引.出于合规性目的，公司必须保留所有输入数据的副本.该公司担心持续成本，并要求解 决方案架构师推荐新的解决方案.

哪种解决方案能够最经济有效地满足这些要求？

1. 将所有数据节点替換为UltraWarm节点以处理预期的容量.当公司将数据加载到集群中时，将输入数据从S3 Standard 转换为 S3 Glacier Deep Archive
2. 将集群中的数据节点数量减少到2个.添加UltraWarm节点以处理预期的容量.配置索引以在OpenSearch服务摄 取数据时转换为UltraWarm.使用S3生命周期策略在1个月后将输入数据转换为S3 Glacier Deep Archive
3. 将集群中的数据节点数量减少到2个.添加UltraWarm节点以处理预期的容量.将索引配置为在OpenSearch服务 摄取数据时转换为UltraWarm.

向集群添加冷存储节点.将索引从UltraWarm转换为冷存储.使用S3生命周期策略在1个月后从S3存储桶中删除输 入数据

1. 将集群中的数据节点数量减少到2个.添加实例文持的数据节点以处理预期的容量.当公司将数据加载到集群中时，将 输入数据从 S3 Standard 转换为 S3 Glacier Deep Archive

答案:C

解析:

Q167.公司使用服务从公司内部托管的应用程序中收集元数据.电视和互联网收音机等消费设备可以访问这些应用程序.许 多旧设备不支持某些HTTP标头，并且当这些标头出现在响应中时会出现错误.该公司配置了一个本地负载平衡器，以从 发送到III设备的响应中删除不受支持的标头，该公司通过User-Agent标头识别这些标头.该公司希望将服务迁移到 AWS.采用无服务器技术.并保留支持旧设备的能力.该公司已经将应用程序迁移到一组AWS Lambda函数中.

哪种解决方案可以满足这些要求？

1. 为元数据服务创建一个Amazon CloudFront分配.创建应用程序负载均衡器(ALB).配*置*CloudFront分配以将请求 转发到ALB.配置ALB以针对每种类型的请求调用正确的Lambda函数.创建CloudFront函数以根据User-Agent标 头的值删除有问题的标头
2. 为元数据服务创建一个Amazon API Gateway REST API.配置API网关为每种类型的请求调用正确的Lambda函 数.修改默认网美响应以根据User-Agent标头的值删除有问题的标头
3. 为元数据服务创建•个Amazon API Gateway HTTP API.fit!置API网关为每种类型的请求调用正确的Lambda函 数.创建响应映射模板以根据User-Agent的值删除有问题的标头.将响应数据映射与HTTP API相关联
4. 为元数据服务创建•个Amazon CloudFront分配.创建应用程序负载均衡器(ALB).配置CloudFront分配以将请求 转发到ALB.配置ALB以针对每种类型的请求调用正确的Lambda函数.创建•个Lambda@Edge函数，该函数将根 据User-Agent标头的值删除有问题的标头以响应査看器请求

答案:A

解析：

Q168.基于软件即服务(SaaS)的公司为客户提供案例管理解决方案.作为该解决方案的一部分，该公司使用独立的简单 邮件传输协议(SMTP)服务器从应用程序发送电子邮件.该应用程序还存储用于确认电子邮件的电子邮件模板，该模板在 应用程序将电子邮件消息发送到之前填充客户数据客户.

该公司计划将此消息传递功能迁移到AWS云，并需要最大限度地减少运营开销.

哪种解决方案能够最经济有效地满足这些要求？

1. 使用来自AWS Marketplace的AMI在Amazon EC2实例上设置SMTP服务器.将电子邮件模板存储在Amazon S3存储桶中.创建•个AWS Lambda函数以从S3存储桶中检索模板并将来自应用程序的客户数据与模板合并.在 Lambda函数中使用SDK发送电子邮件
2. 设置Amazon Simple Email Service (Amazon SES)发送电了邮件.将电子邮件模板存储在Amazon S3存储桶中.创 建•个AWS Lambda函数以从S3存储桶中检索模板并将来自应用程序的客户数据与模板合并.在Lambda函数中使 用SDK发送电子邮件
3. 使用来自AWS Marketplace的AMI在Amazon EC2实例上设置SMTP服务器.使用客户数据参数将电子邮件模 板存储在Amazon Simple Email Service (Amazon SES)中.创建•个AWS Lambda函数来调用SES模板并传递客户 数据以替换参数.使用AWS Marketplace SMTP服务器发送电子邮件
4. 设置Amazon Simple Email Service (Amazon SES)以发送电子邮件.使用客户数据参数将电子邮件模板存储在 Amazon SES上.创建•个AWS Lambda函数来调用SendTemplatedEmail API操作并传递客户数据以替换参数和电 子邮件目的地

答案:D

解析：

Q169.一家公司有一个应用程序作为Amazon Elastic Kubernetes Service (Amazon EKS)集群中多个pod的 ReplicaSet运行.EKS集群在多个可用区中有节点.应用程序生成许多小文件，这些文件必须在应用程序的所有运行实例 中都可以访问.公司需要备份这些文件并将备份保留1年.哪种解决方案能够满足这些要求，同时提供最快的存储性能？

1. 为包含EKS集群中的节点的每个子网创建一个Amazon Elastic File System (Amazon EFS)文件系统和一个挂载 目标.配置ReplicaSet挂载文件系统.指示应用程序将文件存储在文件系统中配置AWS Backup以备份数据副本并将 其保留1年
2. 创建一个 Amazon Elastic Block Store (Amazon EBS)卷.启用 EBS 多重附加功能.

配置ReplicaSet以挂载EBS卷.指示应用程序将文件存储在EBS卷中.配置AWS Backup以备份数据副本并将其保 留1年

1. 创建一个Amazon S3存储桶.配置ReplicaSet以挂载S3存储桶.指示应用程序将文件存储在S3存储桶中.配置 S3版本控制以保留数据副本.配置S3生命周期策略以在1年后删除对象
2. 配置ReplicaSet以使用每个正在运行的应用程序pod t:可用的存储在本地存储文件.使用第三方工具备份EKS集 群1年

答案:C

解析：a