**Vendor:** Amazon

**Exam Code:** AWS Certified Solutions Architect - Professional

**Exam Name:** AWS Certified Solutions Architect - Professional

**Version:** 2020.08.30

【中文版/仅供参考,考试原题请看英文版】

考试是75道题，180分钟

题库覆盖率：90%以上

报名网址：<https://www.aws.training/>

报名考试选中文，英文可以随时参考

Question 1　　　　　**12/12考试原题**

一家公司使用 Amazon 在**单个m4.2xlarge Amazon EC2 实例**上运行遗留系统

EBS2 存储. EC2 实例同时运行Web 服务器和自管理的 Oracle 数据库.每 12 小时对 EBS 卷进行一次快照,并从完全配置的 EC2 实例创建 AMI.最近终止 EC2 实例的事件导致数小时的停机时间.该应用程序已从 AMI 成功启动,但是 EBS 快照的存续时间和数据库的修复导致丢失了 8 个小时的数据.在系统操作员手动执行这些过程的同时,系统也停机了 4 个小时.哪些体系结构更改将最大程度地减少停机时间并减少丢失数据的机会?

1. 创建一个 Amazon CloudWatch 警报以自动恢复实例.创建一个脚本,该脚本将在重新引导后检查并修复数据库.将 Operations 团队订阅到 CloudWatch 警报生成的 Amazon SNS 消息.
2. 在 Elastic Load Balancer / Application Load Balancer 之后的 m4.xlarge EC2 实例上运行应用程序.跨多个可用区在 **Auto Scaling 组中运行 EC2 实例,实例数量最少为 2.**将数据库迁移到 Amazon RDS Oracle Multi-AZ 数据库实例.
3. 在 Elastic Load Balancer / Application Load Balancer 之后的m4.2xlarge EC2 实例上运行应用程序. 在 Auto Scaling 组中运行 EC2 实例,以*最少一个实例*数访问多个可用区.将数据库迁移到 Amazon RDS Oracle Multi-AZ 数据库实例.
4. 将 Web 服务器实例数增加到两个 m4.xlarge 实例,并使用 Amazon Route 53 循环负载均衡来分散负载. 在 Web 服务器上启用 Route 53 健康检查.将数据库迁移到 Amazon RDS Oracle Multi-AZ 数据库实例.

答案: B

解释:

A.不高可用性 C.一个实例仍然不高可用性 D.Route 53 没有循环负载均衡(可能以 50/50 加权).没有自动缩放,它就无法真正扩展.

Question 2 **12/12考试原题 03/09考试原题**

解决方案架构师正在与在 AWS 中运行标准三层 Web 应用程序的公司合作. Web 和应用程序层在Amazon EC2 上运行,数据库层在 Amazon RDS 上运行.该公司正在重新设计 Web 和应用程序层以使用Amazon API Gateway 和 AWS Lambda,并且该公司计划在 6 个月内部署新应用程序. IT 经理已要求解决方案架构师在此期间降低成本.

哪种解决方案在**保持可靠性**的同时最具成本效益?

1. 将竞价型实例用于 Web 层,将按需实例用于应用程序层,并将预留实例用于数据库层.
2. 对 Web 和应用程序层使用**按需实例**,对数据库层使用**保留实例.**
3. 将***竞价型实例***用于 Web 和应用程序层,并将预留实例用于数据库层.
4. 对 Web,应用程序和数据库层使用保留实例.

答案: B

解释:

A.Spot 实例可以被中断 C.Spot 实例可以被中断 D.RI 将需要至少 1 年的租期,在 6 个月后浪费金钱

AWS - 本地网络 DX链接，VPN

VPC - 默认私有网络 访问互联网，按流量收费

EndPoint 终端节点服务 ----通过**VPC 端点（私有隧道 PrivateLink）访问S3，走的是AWS的自己的网络，不收费。 安全。限定只能访问特定的S3存储桶。**

**S3存储桶。:设置存储策略 ，只有特定的用户、角色、安全组可以访问。 类似设定文件夹的访问权限。**

**特定的VPC 端点 ：vpce地址**

S3、RDS ——托管服务，公共服务，互联网公开

Question 3

一家公司使用 Amazon S3 在特定的虚拟私有云(VPC)中存储只能由Amazon EC2 实例访问的文档.该公司担心,有权访问此实例的恶意内部人员还会在另一个 VPC 中设置 EC2 实例来访问这些文档.

以下哪个解决方案将提供所需的保护?

1. 使用 S3 **VPC 端点**和 **S3 存储桶策略**来限制对此 VPC 端点的访问.
2. 使用 EC2 实例配置文件和 S3 存储桶策略来限制对附加到该实例配置文件的角色的访问.
3. 使用 S3 客户端加密并将密钥存储在实例元数据中.
4. 使用 S3 服务器端加密,并使用加密上下文保护密钥.

答案: A

解释:

B.同一角色可以附加到另一个 VPC 中的另一个 EC2 C.实例元数据不是存储密钥的安全位置 D.其他EC2 也可以使用相同的加密上下文

**S3 最适合存储静态图像和视频 搭配cloudfront实现内容分发**

Question 4 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

解决方案架构师管理一个无服务器应用程序,该应用程序由多个 API 网关,AWS Lambda 函数,Amazon S3 存储桶和 Amazon DynamoDB 表组成.客户说,一些应用程序组件在加载**动态图像**时会变慢,而某些则会因" 504 网关超时"错误而超时.在对场景进行故障排除时,解决方案架构师确认 DynamoDB 监视指标处于可接受的水平.

以下哪些步骤对于调试这些应用程序问题将是最佳选择? (选择两个.)

1. Parse HTTP 登录 Amazon API Gateway 中的 HTTP 错误,以确定错误的根本原因.
2. **Parse Amazon CloudWatch Logs 确定在指定时间间隔内请求图像的处理时间.**
3. Parse VPC Flow Logs 确定 Lambda 函数和 S3 之间是否存在数据包丢失.
4. **解析 AWS X-Ray 跟踪并分析 HTTP 方法以确定 HTTP 错误的根本原因.**
5. 解析 S3 访问日志以确定被访问的对象是否来自特定的 IP 地址,以将范围缩小到地理延迟问题. 答案: BD

解释:

A.API 网关 http log(cloudwatch)不能解决根本原因,因为 C.S3 不是基于 VPC 的(除非使用 vpc 端点). Lambda 可以启用 VPC,但此处未提及.动态图像最有可能通过 lambda 函数运行,由 lambda 访问的S3 应该不会出现延迟问题.

DynamoDB :托管NoSql数据库，大量、小数据，低延迟的存储，存储用户的会话信息

IOPS IO的每秒读写次数

Question 5 **12/12考试原题 03/09考试原题**

解决方案架构师正在为最近购买的应用程序设计存储层.该应用程序将在 Amazon EC2 实例上运行,并具有以下层和要求:

-数据层:跨许多系统共享的 **POSIX 文件系统.** -服务层:静态文件内容,需要以 **100k IOPS** 以上的块存储. 哪种 AWS 服务组合可以满足这些需求? (选择两个.)

1. 数据层-Amazon S3 →对象存储
2. Data 层-Amazon EC2 临时存储 →临时存储，本地硬盘 EBS相当于网络外挂硬盘
3. **Data 层-Amazon EFS**
4. Service 层-具有预置 IOPS 的 Amazon EBS 卷
5. Service 层-Amazon EC2 临时存储答案: CE

解释:

A.非 POSIX B.非永久性 D.最大 **EBS IOPS 为 64000**

Question 6

一家公司拥有一个应用程序,该应用程序在 Amazon EC2 实例上运行 Web 服务,并将.jpg 图像存储在Amazon S3 中. Web 流量具有可预测的基线,但是经常会在短期内出现无法预期的峰值.该应用程序是松耦合且无状态的.存储在 Amazon S3 中的.jpg 图像在开始的 15 到 20 天内会经常访问,此**后很少访问,但始终需要立即可用**.首席信息官已要求找到降低成本的方法.

以下哪个选项可以降低成本? (选择两个.)

A.Purchase 预留实例以满足基准容量需求,并使用 On-Demand 实例满足需求高峰. B.**配置生命周期策略,以在 30 天后将 Amazon S3 上的.jpg 图像移动到 S3 IA.**

1. 将按需实例用于基准容量需求,将 Spot Fleet 实例用于需求高峰.
2. 配置生命周期策略,以在 30 天后将Amazon S3 上的.jpg 图像移动到 Amazon Glacier.
3. 创建一个脚本,检查所有 Web 服务器上的负载并终止不必要的按需实例. 答案: AB
4. 解释:
5. Spot 实例的峰值不好,因为可能会中断 D.**Glacier 可能要花费数小时才能访问数据** E.应使用自动缩放组

Question 7 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

公司多年数据中心迁移期间必须使用混合网络体系结构

从多个私有数据中心到 AWS.当前的数据中心与专用光纤链接在一起.由于独特的旧版应用程序,因此无法使用 NAT.在迁移期间,许多应用程序将需要访问数据中心和 AWS 中的其他应用程序.

哪个选项提供安全且**高度可用**的混合网络体系结构,从而允许**高带宽**和**迁移后的多区域部署**?

1. 使用 **AWS Direct Connect 从不同的 ISP 到每个数据中心,**并配置路由以在一个出现故障时故障转移到另一个数据中心的 Direct Connect.确保没有 VPC CIDR 块彼此重叠或内部网络重叠.
2. 使用从本地数据中心到 AWS 的多个硬件 VPN 连接.通过不同的 VPN 连接路由不同的子网流量.确保没有 VPC CIDR 块彼此重叠或内部网络重叠.
3. 在 AWS 和本地数据中心中使用具有集群功能的软件 VPN,并通过集群路由流量.确保没有 VPC CIDR

块彼此重叠或内部网络重叠.

1. 使用 AWS Direct Connect 和 VPN 作为备份,并将两者配置为使用相同的虚拟专用网关和 BGP.确保没有 VPC CIDR 块彼此重叠或内部网络重叠.

答案: A

解释:

不是高带宽 C.一个 VPN 连接不是 HA(群集仍具有一个连接)D.作为备份,VPN 不足以提供高带宽.另外,如果具有虚拟专用网关的区域出现故障怎么办?

Question 8 **11/19考试原题 03/23考题**

一家公司当前在 I / O 密集型的 AWS 上运行生产工作负载.它的工作负载由一个包含 10 个 c4.8xlarge 实例的单层组成,每个实例具有 **2 TB gp2 卷**.最近处理作业的数量增加了,延迟也增加了.团队意识到他们受到 IOPS 的限制.为了使应用程序高效运行,他们需要为每个实例将 IOPS 增加 3,000.

以下哪个设计可以最有效地满足 MOST 的性能目标?

1. 将 Amazon EBS 卷的类型从 gp2 更改为io1,并将预配置的IOPS 设置为 9,000.
2. **将每个实例中的 gp2 卷的大小增加到 3 TB.**
3. 创建一个新的 Amazon EFS 文件系统,并将所有数据移动到该新文件系统.将此文件系统挂载到所有 10

个实例.

1. 创建一个新的 Amazon S3 存储桶,并将所有数据移动到该新存储桶.允许每个实例访问此 S3 存储桶并将其用于存储.

答案: B

解释:

A.成本将为 3000 \* 0.125 + 9000 \* 0.065 B.成本将为 3000 \* 0.1(**gp2 每 GB 具有 3 IOPS**)C.EFS 的延迟

高 于 EBS 设 置 的 IOPS https://docs.aws.amazon.com/efs/latest/ug/performance.html S3 在 IO 方面不如 EBS 快

Question 9

公司的数据中心通过最少使用的 **10 Gbps** AWS Direct Connect 连接连接到 AWS Cloud,该连接具有到其虚拟**私有云(VPC)的私有虚拟接口**.公司的互联网连接速度为 200 Mbps,并且公司**每个星期五都有 150 TB 的数据集被创建**.数据必须在星期一早上在 Amazon S3 中传输并可用.

在允许数据传输增长的同时,满足需求的最昂贵的方法是哪一种?

1. 订购两个 80 GB 的 AWS Snowball 设备.将数据卸载到设备,然后将其发送到 AWS. AWS 会将数据从 Snowball 设备复制到 Amazon S3.
2. 为 Amazon S3 创建 VPC 终端节点.使用 VPC 终端节点将数据复制到 Amazon S3,***强制传输***使用直接连接.
3. 为 Amazon S3 创建 VPC 终端节点.在 VPC 中的经典负载均衡器后面设置***反向代理服务***器场.使用代理将数据复制到 Amazon S3.
4. 在 Direct Connect 连接上创建**公共虚拟接口**,然后通过该连接将数据复制到 **Amazon S3.**

答案: D

解释:

A.不够快 B.S3 **VPC 终结点**是网关终结点,不能跨直接连接扩展https://docs.amazonaws.cn/zh\_CN/vpc/latest/userguide/vpce-gateway.html#Gateway-Endpoint- Limitations

C.Proxy 比 D 贵

Question 10

一家公司为各个开发团队创建了一个帐户,**总共有 200 个帐户**.所有帐户在单个区域中都有一个虚拟私有云(VPC),并且在 Docker 容器中运行多个微服务,这些服务需要与其他帐户中的微服务进行通信.安全团队的要求指出,这些微服务不得穿越公共互联网,并且仅应允许某些内部服务调用其他单个服务.如果服务的网络流量被拒绝,则必须将任何拒绝的请求(包括源 IP)通知安全团队.

在满足安全性要求的同时,如何在服务之间建立连接?

1. ***在 VPC 之间创建 VPC 对等连接.***在实例上使用安全组,以允许来自允许调用微服务的安全组 ID 的流量. 将网络 ACL 应用到本地 VPC,并仅允许来自本地 VPC 和对等 VPC 的流量.在 Amazon ECS 中针对每个微服务的任务定义中,使用 awslogs 驱动程序指定日志配置.在 Amazon CloudWatch Logs 中,创建指标过滤器,并警告HTTP 403 响应数量.当邮件数量超过安全团队设置的阈值时,创建警报.
2. 确保没有 CIDR 范围重叠,并将虚拟专用网关(VGW)附加到每个 VPC.

在每个 VGW 之间设置 IPsec 隧道,并在路由表上启用路由传播.在每个服务上配置安全组,以允许其他帐户上的 VPC 的 CIDR 范围.启用 VPC 流日志,并使用Amazon CloudWatch Logs 订阅过滤器处理拒绝的流量.创建一个 IAM 角色,并允许安全团队为每个帐户调用 AssumeRole 操作.

1. 通过使用在 Amazon EC2 上运行的***第三方市场 VPN 设备***,在 VPN 设备与该区域内每个 VPC 附加的虚拟专用网关(VGW)之间动态路由的 VPN 连接来部署中转 VPC.调整网络 ACL,以仅允许来自本地 VPC 的流量.将安全组应用于微服务,以仅允许来自 VPN 设备的流量.

在每个 VPN 设备上安装 awslogs 代理,并配置日志以转发到安全帐户中的 Amazon CloudWatch Logs,以供安全团队访问.

1. 为**每个微服务创建一个网络负载平衡器(NLB).**将 NLB 附加到 PrivateLink 终结点服务,并将将使用此服务的帐户列入白名单.在使用者 VPC 中创建一个接口终结点,并关联一个安全组,该安全组仅允许被授权调用生产者服务的服务的安全组 ID.在生产者服务上,为每个微服务创建安全组,并仅允许 CIDR 范围允许的服务.在每个 VPC 上创建 VPC 流日志,以捕获将传递到 Amazon CloudWatch Logs 组的拒绝流量.

创建将日志数据流式传输到安全帐户的 CloudWatch Logs 订阅.

答案: D

解释:

1. 不会拒绝 HTTP 403 请求,因为该请求将永远不会到达 ECS VPC 对等方将保留原始 IP(因此不允许CIDR 重叠)
2. 登录多个帐户不是最佳实践.此外,如果 VPC 中只有两个服务之一应访问特定的微服务,则这将无法正常工作,因为 SG 允许整个 VPC VPN 保留原始 IP,除非在进入隧道的流量之前使用 NAT
3. 所有流量都流向同一 VPN 设备,这意味着实际上无法阻止服务访问. ACL 仅允许本地 VPC,而转接VPC 将不起作用.
4. 这将不起作用,因为 PrivateLink 将使用本地 VPC 的专用IP 创建服务端点,这意味着您将没有源 IP,并且生产者中的安全组无法范围允许的服务. https://docs.aws.amazon.com/whitepapers/latest/aws-vpc- connectivity-options/aws-privatelink.html 但是,当消费者 VPC 上的服务被拒绝时,日志应具有 VPC 端点. 但是,在生产者端允许的 IP 很棘手.我认为这意味着同一 VPC 中允许的服务.无论如何,我认为这是唯一有意义的解决方案,即使其中有很多模糊的描述

Question 11 **11/19考试原题 03/23考题**

一家公司运行的动态关键任务 Web 应用程序的 SLA 为 99.99%.全局应用程序用户 24/7 访问应用程序. 该应用程序当前托管在内部,通常无法满足其 SLA,尤其是**当数百万用户**同时访问该应用程序时.**远程用户抱怨延迟.**

应如何重新设计此应用程序以使其具有可伸缩性,并以最低的成本实现自动故障转移?

1. 将 Amazon Route 53 故障转移路由与***基于地理位置的路由一***起使用.在每个应用程序负载均衡器后面自动缩放的 Amazon EC2 实例上托管网站,并为每个区域中的应用程序层提供附加的 Application Load Balancer 和 EC2 实例.将多可用区部署与 MySQL 用作数据层.
2. 使用 Amazon Route 53 ***循环路由,***通过运行状况检查将负载平均分配到几个区域.将网站托管在具有网络负载均衡器后面的 AWS Fargate 技术容器的自动缩放的 Amazon ECS 上,并在每个区域中为应用程序层提供额外的 Network Load Balancer 和 Fargate 容器.将 Amazon Aurora 副本用于数据层.
3. 使用基于 Amazon Route 53 的**基于延迟的路由通过运行状况检查路**由到最近的区域.在每个区域的**Amazon S3 中托管网站**,并将 **Amazon API Gateway 与 AWS Lambda** 一起用于应用程序层.将 Amazon **DynamoDB 全局表**与 Amazon DynamoDB Accelerator**(DAX**)一起用作数据层进行缓存.
4. 使用基于 Amazon Route 53 ***地理位置的路由***.将网站托管在网络负载均衡器后面的自动缩放的 AWS Fargate 容器上,并为每个区域中的应用程序层提供额外的 Network Load Balancer 和 Fargate 容器.使用适用于 Aurora MySQL 的 Amazon Aurora Multi-Master 作为数据层.

答案: C

解释:

A.这将比 C 更昂贵.B. Route 53 循环路由不是NLB 不支持粘性会话的事情,Web 应用程序很可能需要一个 C.**使用托管服务是最佳实践. S3,Lambda 和 DynamoDB 比 EC2 和 RDS**  **便宜得多**.DNLB 不支持Sticky 会话,并且 Multi Master 无法跨区域

Question 12 **03/23考题**

一家公司管理 200 多个单独的面向互联网的 Web 应用程序.所有应用程序都部署在单个AWS 区域中的AWS 上.所有应用程序的完全限定域名(FQDN)可通过使用应用程序负载平衡器(ALB)的 HTTPS 获得. ALB 配置为使用公共 SSL / TLS 证书.

解决方案架构师需要将 Web 应用程序迁移到多区域架构.所有 HTTPS 服务都应继续工作而不会中断. 哪种方法满足这些要求?

1. 使用 AWS KMS 为每个 FQDN 申请证书.将证书与主要AWS 区域中的 ALB 关联.在 AWS KMS 中为证书启用跨区域可用性,并将证书与辅助 AWS 区域中的 ALB 关联.
2. 使用 AWS KMS 为每个 FQDN 生成密钥对和证书请求.将证书与主要和辅助AWS 区域中的 ALB 关联.
3. 使用 AWS Certificate Manager 为每个 FQDN 申请证书.将证书与主要和辅助 AWS 区域中的 ALB 关联.
4. 使用 **AWS Certificate Manager** 为主要和辅助 AWS 区域中的每个 FQDN 请求证书.将证书与每个

AWS 区域中的相应 ALB 关联.

答案: D

解释:

A.KMS 不适用于证书 B.KMS 不适用于证书 C.**ELB 的证书不能跨区域**

https://aws.amazon.com/certificate-manager/faqs/

Question 13 **12/12考试原题 03/09考试原题**

一家电子商务公司正在改造其 IT 基础架构,并计划使用 AWS 服务.该公司的 CIO 已要求解决方案架构师设计一个简单,**高度可用且松散耦合**的订单处理应用程序.在将订单存储在 Amazon DynamoDB 表中之前, 该应用程序负责接收和处理订单.**该应用程序具有零星的流量模式,**应该能够在市场营销活动期间扩展,以最小的延迟处理订单.

满足要求的**最可靠**的方法是以下哪项?

1. 在 Amazon EC2 托管的数据库中接收订单,并使用EC2 实例进行处理.
2. **在 Amazon SQS 队列中接收订单,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 容器进行处理.
4. 在 Amazon Kinesis Data Streams 中接收订单,并使用 Amazon EC2 实例对其进行处理.

答案: B

解释:

A.真的不好. B.Lambda 函数更可靠且可扩展 C.这不是步进函数的作用 D.需要配置自动缩放,并且运动学没有项目级别的确认

Question 14 **12/12考试原题**

公司拥有使用内部软件框架编写的应用程序.框架安装需要 30 分钟,并使用用户数据脚本执行.公司开发人员经常将更改部署到应用程序.框架安装正在成为此过程的瓶颈.

以下哪项将加速此过程?

A.创建一个管道来构建安装了框架的自定义 AMI,并将该 AMI 用作应用程序部署的基准. B.使用用户数据脚本安装框架,但压缩安装文件以使其更小.

1. 创建一个管道以并行化安装任务,并从用户数据脚本中调用该管道.
2. 配置一个 AWS OpsWorks 食谱, 该食谱将安装框架而不是使用用户数据.

将此手册用作所有部署的基础.

答案: A

解释:

B.安装不能并行化. C.安装不能并行化. D.Cookbook 是收据的集合,我认为这里应该是收据.但是,这仍然需要运行安装,并且不会缩短时间

Question 15 **12/12考试原题 03/09考试原题**

一家公司希望确保其每个业务部门的工作负载具有完全的自主权,并且在 AWS 中具有最小的爆炸半径.安全团队必须能够控制对帐户中资源和服务的访问,以确保业务部门不会使用特定的服务.

解决方案架构师如何达到隔离要求?

1. 为每个业务部门创建单独的账户,并将该账户添加到 AWS Organizations 中的 OU.修改 OU 以确保特定服务被阻止.通过 IdP 联合每个帐户,并为业务部门和安全团队创建单独的角色.
2. 为每个业务部门创建个人帐户.通过 IdP 联合每个帐户,并为业务部门和安全团队创建单独的角色和策略.
3. 为整个公司创建一个共享帐户.为每个业务部门创建单独的VPC.

为每个业务部门创建单独的 IAM 策略和资源标签.通过 IdP 联合每个帐户,并为业务部门和安全团队创建单独的角色.

1. 为整个公司创建一个共享帐户.为每个业务部门创建单独的IAM 策略和资源标签.通过 IdP 联合帐户,并为业务部门和安全团队创建单独的角色.

答案: A

解释:

A.最佳实践,具有最小的爆炸半径和自主权

Question 16 **12/12考试原题 03/09考试原题**

一家公司正在从 Amazon EC2 实例迁移其部分应用程序 API,以在无服务器基础架构上运行.该公司已为新应用程序设置了 Amazon API Gateway,AWS Lambda 和 Amazon DynamoDB. Lambda 函数的主要职责是从第三方软件即服务(SaaS)提供程序获取数据.为了保持一致性,Lambda 函数被附加到与原始EC2 实例相同的虚拟私有云(VPC).

测试用户报告无法使用此新迁移的功能,并且该公司从API Gateway 收到 5xx 错误.来自 SaaS 提供商的监视报告显示,请求从未发送到其系统.该公司注意到Lambda 函数正在生成 Amazon CloudWatch Logs. 当针对 EC2 系统测试相同功能时,它会按预期工作.

是什么原因引起的?

A.Lambda 所在的子网中没有连接到 SaaS 提供程序的 NAT 网关. B.最终用户应用程序配置错误,无法继续使用EC2 实例支持的端点. C.在 API 网关上设置的限制阈值太低,请求没有通过.

D. API 网关没有必要的权限来调用 Lambda.

答案: A

解释:

B.有 Lambda 日志 C.如果是这种情况,则某些请求将有效 D.有 lambda 日志

Question 17 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

解决方案架构师正在与一家对其 IT 成本极为敏感的公司合作,并希望实施控制措施,以实现每月可预测的

AWS 支出.

哪些步骤组合可以帮助公司控制和监视其每月的 AWS 使用量,以使成本尽可能接近目标金额? (选择三个.)

1. 实施 IAM 策略,要求用户在启动 Amazon EC2 实例时指定"工作负载"标签以进行成本分配.
2. 联系 AWS 支持人员,并要求他们将限制应用于该帐户,以使用户不能启动超过一定数量的实例类型. C.购买所有预备预留实例,这些实例可满足该帐户的预期 Amazon EC2 使用量的 100%.
3. 在用户的 IAM 策略中放置条件,以限制他们能够启动的实例数量.
4. 在 AWS Billing and Cost Management 控制台中将"工作量"定义为成本分配标签.
5. 设置 AWS 预算,以在给定工作负载超过预期成本时发出警报和通知.

答案: AEF

解释:

A.aws:RequestTag/tag-key B.不正确的做法 C.不起作用,因为这可能会增加成本 D.IAM 不支持此

https://forums.aws.amazon.com/thread.jspa?threadID = 174503

Question 18

一家大型跨国公司希望将无状态的关键任务应用程序迁移到 AWS.该应用程序基于 z / OS 操作系统上的

IBM WebSphere(应用程序和集成中间件),IBM MQ(消息中间件)和 IBM DB2(数据库软件).

解决方案架构师应如何将应用程序迁移到 AWS?

1. 通过 Auto Scaling 在负载均衡器后面的 Amazon EC2 上重新托管基于 WebSphere 的应用程序.

将 IBM MQ 重新平台化为基于 Amazon EC2 的 MQ.将基于 z / OS 的 DB2 重新平台化为Amazon RDS DB2.

1. 通过 Auto Scaling 在负载均衡器后面的 Amazon EC2 上重新托管基于 WebSphere 的应用程序.

将 IBM MQ 重新平台化为 Amazon MQ.将基于 z / OS 的 DB2 重新平台化为基于 Amazon EC2 的 DB2. C.使用 AWS Elastic Beanstalk 编排和部署应用程序.将 IBM MQ 重新平台化为 Amazon SQS.将基于z / OS 的 DB2 重新平台化为 Amazon RDS DB2.

D.使用 AWS Server Migration Service 将 IBM WebSphere 和 IBM DB2 迁移到基于 Amazon EC2 的解决方案.将 IBM MQ 重新平台化为 Amazon MQ.

答案: B

解释:

A.RDS 不支持 DB2 C.RDS 不支持DB2 D.Server MIgration Service 与 VM 一起使用,并且没有提及VM,SMS 仅支持 Linux 和 Windows https://docs.aws.amazon.com/server-migration -service / latest / userguide / prereqs.html＃os\_prereqs

Question 19 **12/12考试原题**

媒体存储应用程序将用户照片上传到 Amazon S3 进行处理.最终用户报告某些上传的照片未得到正确处理.应用程序开发人员跟踪日志,并发现当同时有数千个用户同时在系统上时,AWS Lambda 遇到执行问题. 问题是由以下原因引起的:

-限制并发执行.

-保存数据时 Amazon DynamoDB 的性能.

可以采取哪些措施来提高应用程序的性能和可靠性? (选择两个.) A.评估并调整 DynamoDB 表的读取容量单位(RCU).

1. 评估并调整 DynamoDB 表的写入容量单位(WCU).
2. 添加一个 Amazon ElastiCache 层以提高 Lambda 函数的性能. D.配置一个死信队列,它将重新处理失败或超时的 Lambda 函数. E.使用 S3 传输加速为最终用户提供较低延迟的访问.

答 案 : BD Question 20

一家公司经营着一组成像卫星.卫星将数据流传输到该公司的一个地面站,在该地面站进行处理每分钟可 产生约 5 GB 的图像.将此数据添加到网络连接的存储中,其中已经存储了 2 PB 的数据.

该公司经营着一个网站,允许其客户访问和购买图片

互联网.该网站也在地面站上运行.使用情况分析表明,客户最有可能访问最近 24 小时内捕获的图像. 该公司希望将映像存储和分发系统迁移到 AWS,以降低成本并增加可以服务的客户数量.

哪种 AWS 架构和迁移策略将满足这些要求?

1. 使用多个 AWS Snowball 设备将现有图像迁移到 Amazon S3.创建一个从地面站到 AWS 的 1-Gb AWS Direct Connect 连接,并将新数据上传到

Amazon S3 通过 Direct Connect 连接.将数据分发网站迁移到 Amazon EC2 实例.通过使用 Amazon S3

作为来源,让此网站通过创建签名的 URL 通过 Amazon CloudFront 提供数据.

1. 创建一个从地面站到 AWS 的 1-Gb Direct Connect 连接.使用 AWS Command Line Interface 通过

AWS 命令行界面复制现有数据并将新数据上传到 Amazon S3

直接连接.将数据分发网站迁移到 EC2 实例.通过使用 Amazon S3 作为来源,让该网站通过创建签名的

URL 通过 CloudFront 提供数据.

1. 使用多个 Snowball 设备将现有图像迁移到 Amazon S3.通过定期使用 Snowball 设备从网络连接的存储中上传数据来上传新数据.将数据分发网站迁移到 EC2 实例.通过使用 Amazon S3 作为来源,让该网站通过创建签名的 URL 通过 CloudFront 提供数据.
2. 使用多个 Snowball 设备将现有映像迁移到 Amazon EFS 文件系统.创建从地面站到 AWS 的 1-Gb Direct Connect 连接,并通过在 Direct Connect 连接上挂载 EFS 文件系统来上传新数据.将数据分发网站迁移到 EC2 实例.通过在 EC2 中使用将 EFS 文件系统挂载为源的 Web 服务器,使该网站通过创建签名的URL 通过 CloudFront 为数据提供服务.

答案: A

解释:

B.1GB(用于 2PB)将太慢 C.Snowball 无法确保最近 24 小时的数据可用 D.EFS 在这种情况下价格昂贵

Question 21

公司提取并处理流式市场数据.数据速率是恒定的.每晚运行一个计算聚合统计信息的过程,每次执行大约 需要 4 个小时才能完成.统计分析对业务而言不是关键任务,如果特定运行失败,则在下次执行时获取先前的数据点.

当前架构使用具有全天候运行 1 年保留的 Amazon EC2 预留实例池来提取流数据并将其存储在附加的Amazon EBS 卷中.每天晚上启动按需 EC2 实例以执行每晚处理,从摄取服务器上的 NFS 共享访问存储的数据,并在完成后终止每晚处理服务器.预留实例预留即将到期,并且公司需要确定是购买新预留还是实 施新设计.

哪个是最具成本效益的设计?

1. 更新摄取过程以使用 Amazon Kinesis Data Firehose 将数据保存到Amazon S3.使用按需运行的 EC2

实例队列,该实例每天晚上启动以执行 S3 数据的批处理,并在处理完成时终止.

1. 更新摄取过程以使用 Amazon Kinesis Data Firehouse 将数据保存到 Amazon S3.使用 AWS Batch 以按需价格的 50%的现货市场出价执行每晚处理.
2. 更新提取过程,以使用网络负载平衡器(含 3 年租约)后面的 EC2 预留实例队列.将批处理竞价型实例与夜间处理的最高出价为按需价格的 50%一起使用.
3. 更新摄取过程以使用 Amazon Kinesis Data Firehose 将数据保存到 Amazon Redshift.

使用排定在每晚与 Amazon CloudWatch Events 一起运行的 AWS Lambda 函数来查询 Amazon Redshift 以生成每日统计信息.

答案: B

解释:

A.比 B 贵.B.因为它不是关键任务,可以从先前的数据点提取数据,所以 Spot 实例很有意义 C.如果我们仍然使用 EBS,则每个实例将拥有自己的 EBS,并且数据难以汇总. EC2 也很昂贵 D.Lambda 的过程限制为15 分钟

Question 22 **12/12考试原题** **11/19考试原题**

三层 Web 应用程序在 Amazon EC2 实例上运行. Cron 守护程序用于触发收集 Web 服务器,应用程序和数据库日志并将其每小时发送到集中位置的脚本.有时,扩展事件或计划外中断导致实例在收集最新日志之前停止,并且日志文件丢失.

以下哪个选项是收集和保留日志文件的最可靠的方法?

1. 将 cron 更新为每 5 分钟而不是每小时运行一次,以减少因中断而丢失日志消息的可能性.
2. 使用 Amazon CloudWatch Events 触发 Amazon Systems Manager 运行命令,以更频繁地调用日志收集脚本,以减少因中断而丢失日志消息的可能性.
3. 使用 Amazon CloudWatch Logs 代理将日志消息直接流式传输到 CloudWatch Logs.将代理的批处理计数配置为 1,以减少因中断而丢失日志消息的可能性.
4. 使用 Amazon CloudWatch Events 触发 AWS Lambda SSH 进入每个正在运行的实例,并更频繁地调用日志收集脚本,以减少因中断而丢失日志消息的可能性.

答案: C

解释:

几乎没有延迟.最可靠

**先匹配长**

的123.123.123.123/32 →最小IP段，就一个

123.0.0.0/8 →前面8位固定 ，2的24次方个IP地址的IP段

Question 23 **12/12考试原题 03/09考试原题**

公司将销售交易数据存储在 Amazon DynamoDB 表中.要检测异常行为并快速响应,必须在 30 分钟内记录对 DynamoDB 表中存储的项目的所有更改.

哪种解决方案符合要求?

1. 每小时将 DynamoDB 表复制到 Amazon EMR 上的 Apache Hive 表中,并分析它们的异常行为.当检测到异常行为时,发送 Amazon SNS 通知.
2. 使用 AWS CloudTrail 捕获更改 DynamoDB 表的所有 API.使用 CloudTrail 事件过滤检测到异常行为时发送 SNS 通知.
3. 使用 Amazon DynamoDB 流捕获和发送更新到 AWS Lambda.创建 Lambda 函数以将记录输出到Amazon Kinesis Data Streams.使用 Amazon Kinesis Data Analytics 分析任何异常.当检测到异常行为时发送 SNS 通知.
4. 使用 Amazon CloudWatch Events 中的事件模式以 AWS Lambda 函数为目标来捕获 DynamoDB API

调用事件以分析行为.当检测到异常行为时发送 SNS 通知.

答案: C

解释:

B.我们要跟踪项目更改,而不是表更改C.最佳实践 D.DynamoDB 不被 cloudwatch 事件支持,您将需要

cloudtrail

Question 24 **12/12考试原题**

一家公司正在 Amazon EC2 上运行多个应用程序.每个应用程序均由多个业务部门部署和管理.所有应用程序均部署在单个 AWS 账户上,但部署在不同的虚拟私有云(VPC)上.该公司在同一帐户中使用单独的VPC 进行测试和开发.

当用户意外终止和修改属于另一个业务部门的资源时,生产应用程序将遭受多次中断.已要求解决方案架 构师改善公司应用程序的可用性,同时允许开发人员访问所需的资源.

哪个选项符合最小中断要求?

1. 为每个业务部门创建一个 AWS 账户.将每个业务部门的实例移至其自己的帐户,并建立联盟以允许用户访问其业务部门的帐户.
2. 设置联盟以允许用户使用他们的公司凭据,并将用户锁定到自己的 VPC.使用网络 ACL 阻止每个 VPC

访问其他 VPC.

1. 实施基于业务部门的标记策略.创建 IAM 策略,以便每个用户只能终止属于自己业务部门的实例. D.为每个用户设置基于角色的访问权限,并基于各个角色和每个用户负责的服务提供有限的权限.

答案: D

解释:

A.跨帐户移动实例会导致中断 B.将停止服务间通信 C.将不满足开发和测试实例的需要Question 25 **12/12考试原题 03/09考**

企业在本地数据中心的虚拟机上运行 103 个业务线应用程序.许多应用程序是简单的 PHP,Java 或 Ruby Web 应用程序,不再被积极开发,并且流量很少.

应使用哪种方法以最低的基础架构成本将这些应用程序迁移到 AWS?

A.将应用程序部署到没有负载均衡器的单实例 AWS Elastic Beanstalk 环境中. B.使用 AWS SMS 为每个虚拟机创建 AMI,然后在Amazon EC2 中运行它们.

1. 将每个应用程序转换为 Docker 映像,然后部署到 Application Load Balancer 后的小型 Amazon ECS

集群.

1. 使用 VM Import / Export 为每个虚拟机创建 AMI,并通过配置自定义映像在单实例 AWS Elastic Beanstalk 环境中运行它们.

答案: C

解释:

A.103 EC2 仍然需要 B.103 EC2 C.我们可以在一个小型 EC2 中运行所有 ECS 容器并使用 ALB 进行路由,这确实非常便宜 D.103 EC2

Question 26

解决方案架构师必须为公司专有和敏感应用程序的 500MB 源代码存储库创建具有成本效益的备份解决方案.该存储库在 Linux 上运行,每天备份到磁带.磁带备份存储 1 年.

当前的解决方案不能满足公司的需求,因为它是一个容易出错,维护成本高并且不满足 1 小时的恢复点目

标(RPO)或 1 小时的恢复时间目标(RTO)的手动过程. 2 小时.新的灾难恢复要求是将备份存储在异地并能够在需要时还原单个文件.

哪种解决方案能以最少的努力和费用满足客户对 RTO,RPO 和灾难恢复的需求?

1. 用 AWS Storage Gateway 虚拟磁带库替换本地磁带以与当前备份软件集成.每晚运行备份,并将虚拟磁带存储在 US-EAST-1 中的 Amazon S3 标准存储上.使用跨区域复制在 US-WEST-2 中创建第二个副本. 使用 Amazon S3 生命周期策略执行自动迁移到 Amazon Glacier 并在 1 年后删除过期的备份吗?
2. 配置本地源代码存储库以将文件同步到 AWS Storage Gateway 文件 Amazon 网关,以将备份副本存储在 Amazon S3 Standard 存储桶中.在 Amazon S3 存储桶上启用版本控制.创建 Amazon S3 生命周期策略以将对象的旧版本自动迁移到 Amazon S3 Standard 0 Infrequent Access,然后迁移到 Amazon Glacier,然后在 1 年后删除备份.
3. 用存储网关存储卷替换本地源代码存储库存储.将默认快照频率更改为 1 小时.使用 Amazon S3 生命周期策略将快照存档到 Amazon Glacier,并在 1 年后删除旧快照.使用跨区域复制在 US-WEST-2 中创建快照的副本.
4. 用存储网关缓存卷替换本地源代码存储库存储.创建快照计划以进行每小时快照.使用 Amazon CloudWatch Events 调度表达式规则在每小时的 AWS Lambda 任务上运行,以将快照从 US-EAST -1 复制到 USWEST-2.

答案: B

解释:

A.无法满足 1 小时的 RPO C.Volume 网关存储快照,不允许还原单个文件

https://aws.amazon.com/storagegateway/faqs

Question 27 **11/19考试原题**

公司的 CFO 最近分析了公司的 AWS 每月账单,并确定了降低使用 AWS Elastic Beanstalk 环境成本的机会. CFO 已要求解决方案架构师设计一个高度可用的解决方案,该解决方案将在早上启动 Elastic Beanstalk 环境,并在一天结束时终止该环境.

该解决方案的设计应以最小的运营开销并最大程度地降低成本.它还应该能够处理不同团队之间对Elastic Beanstalk 环境的更多使用,并且必须为所有团队提供一站式调度程序解决方案,以保持较低的运营成本.

什么设计可以满足这些要求?

1. 设置一个 Linux EC2 Micro 实例.配置 IAM 角色以允许启动和停止 Elastic Beanstalk 环境并将其附加到实例.在实例上创建脚本以启动和停止 Elastic Beanstalk 环境.在实例上配置 cron 作业以执行脚本.
2. 开发 AWS Lambda 函数以启动和停止 Elastic Beanstalk 环境.配置一个 Lambda 执行角色,以授予Elastic Beanstalk 环境启动/停止权限,然后将该角色分配给 Lambda 函数.配置 cron 表达式 Amazon CloudWatch Events 规则以触发 Lambda 函数.
3. 开发一个以" wait"为类型的 AWS Step Functions 状态机,以控制启动和停止时间.

使用活动任务来启动和停止 Elastic Beanstalk 环境.为"步骤功能"创建角色,以允许其启动和停止 Elastic Beanstalk 环境.每天调用步进功能.

1. 配置一个基于时间的 Auto Scaling 组.早晨,让 Auto Scaling 组扩展 Amazon EC2 实例,并将 Elastic Beanstalk 环境启动命令放入 EC2 实例用户日期.在一天结束时,将实例编号缩减为 0 以终止 EC2 实例.

答案: B

解释:

1. 需要一直运行 EC2 B.推荐的解决方案https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/ C.Step 函数不用于此目的,而具有 step 函数的角色将无助于工作者任务.

D.EC2 需要在日期时间运行..并不是很好的解决方案

Question 28 **12/12考试原题 03/09考试原题**

一家公司计划将受监管和对安全敏感的业务迁移到 AWS.安全团队正在开发一个框架,以验证 AWS 最佳实践和行业认可的合规性标准的采用. AWS 管理控制台是团队配置资源的首选方法.

解决方案架构师应使用哪些策略来满足业务需求并持续评估,审核和监视 AWS 资源的配置? (选择两个.) A.使用 AWS Config 规则定期审核对 AWS 资源的更改并监视配置的合规性.使用 AWS Lambda 开发

AWS Config 自定义规则以建立测试驱动的开发方法,并根据所需控件进一步自动评估配置更改.

1. 使用 Amazon CloudWatch Logs 代理收集所有 AWS 开发工具包日志.使用一组预定义的过滤器模式搜索日志数据,该模式会机器化 API 调用.当执行意外更改时,使用 Amazon CloudWatch 警报发送通知.通过将批处理导出到 Amazon S3,然后再导出到 Amazon Glacier,可以存档日志数据,以实现长期保留和可审核性.
2. 使用 AWS CloudTrail 事件评估所有AWS 账户的管理活动.确保在所有帐户和可用的 AWS 服务中启用 CloudTrail.启用跟踪,加密

带有 AWS KMS 密钥的 CloudTrail 事件日志文件,并使用 CloudWatch Logs 监视记录的活动.

1. 使用 Amazon CloudWatch Events 近实时功能来监视系统事件模式,并触发AWS Lambda 函数以自动还原 AWS 资源中的未经授权的更改.

另外,以 Amazon SNS 主题为目标,以启用通知并缩短事件响应的响应时间.

1. 将 CloudTrail 与 Amazon SNS 集成使用以自动通知未经授权的 API 活动.确保在所有帐户和可用的

AWS 服务中启用 CloudTrail.评估 Lambda 函数的使用情况,以自动还原 AWS 资源中未经授权的更改.

答案: AC

解释:

B.管理控制台不要通过 SDK.D.需要 cloudtrail 将资源更改记录到 cloudwatch E.Cloudtrail 到 SNS 没有过滤,因此您需要发送所有日志. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure- sns-notifications-for- cloudtrail.html＃configure-cloudtrail-to-send-notifications

Question 29 **11/19考试原题**

一家公司正在内部运行高用户量的媒体共享应用程序.目前,它托管着约 400 TB 的数据以及数百万个视频文件.该公司正在将该应用程序迁移到 AWS,以提高可靠性并降低成本.

解决方案架构团队计划将视频存储在 Amazon S3 存储桶中,并使用Amazon CloudFront 将视频分发给用户.该公司需要将该应用程序迁移到 AWS 至少 10 天,并尽可能减少停机时间.该公司目前具有 1 Gbps 的Internet 连接能力,并具有 30%的可用容量.

以下哪种解决方案可使公司将工作负载迁移到 AWS 并满足所有要求?

1. 在 Amazon S3 客户端中使用分段上传,以通过 Internet 将数据并行上传到 Amazon S3 存储桶.使用限制功能以确保 Amazon S3 客户端使用的可用互联网容量不超过 30%.
2. 请求将具有 1 PB 容量的 AWS Snowmobile 交付给数据中心.将数据加载到 Snowmobile 并发送回去, 以使 AWS 将数据下载到 Amazon S3 存储桶.同步在迁移过程中生成的新数据.
3. 使用 Amazon S3 客户端通过 Internet 将数据从数据中心传输到 Amazon S3 存储桶.使用限制功能以确保 Amazon S3 客户端使用的可用互联网容量不超过 30%.
4. 请求将多个 AWS Snowball 设备交付到数据中心.同时将数据加载到这些设备中并发送回去.让 AWS

将数据下载到 Amazon S3 存储桶.同步在迁移过程中生成的新数据.

答案: D

解释:

A.需要 123 天.. Parralel 仍然具有互联网连接,因为瓶颈 B.建议将雪上移动设备的温度超过 10PB C.需要123 天的时间.

Question 30 **12/12考试原题** **11/19考试原题**

一家公司开发了一个新的计费应用程序,该应用程序将在两周内发布.

开发人员正在使用 CIDR 块 172.31.0.0/16 在 VPC A 子网 172.31.0.0/24 中由 Auto Scaling 组管理的 10 个 EC2 实例上运行的应用程序进行测试.开发人员在使用 CIDR 块 172.50.0.0/16 连接到 VPC B 中同一区域中的 Amazon EC2 实例上运行的 Oracle 数据库时,发现了应用程序日志中的连接超时错误.数据库实例的 IP 在应用程序实例中进行了硬编码.

解决方案架构师应向开发人员提出哪些建议,以最少的维护和开销以安全的方式解决问题?

1. 对运行该应用程序和 Oracle 数据库的所有实例禁用 SrcDestCheck 属性.将 VPC A 的默认路由更改为指向 IP 地址在 172.50.0.0/26 范围内的 Oracle 数据库的 ENI
2. 为两个 VPC 创建并附加 Internet 网关.为两个 VPC 配置到 Internet 网关的默认路由.为 VPC A 中的每个 Amazon EC2 实例分配一个弹性 IP
3. 在两个 VPC 之间创建一个 VPC 对等连接,并将路由添加到 VPC A 的路由表,该路由指向 IP 地址范围

172.50.0.0/16

1. 为每个 VPC 创建一个额外的 Amazon EC2 实例作为客户网关；为每个 VPC 创建一个虚拟专用网关

(VGW),配置端到端 VPC,并发布 172.50.0.0/16 的路由

答案: C

解释:

A 这是用于 NAT 吗?它不会有帮助,因为目标是数据库,源将是 EC2 B.数据库连接不应通过 Internet D.传输 VPC 太麻烦了!

Question 31 **11/19考试原题 03/23考题**

已要求解决方案架构师研究公司的 Amazon Redshift 集群,该集群已迅速成为其技术的组成部分并支持关键业务流程.解决方案架构师将提高群集的可靠性和可用性,并提供选项以确保出现问题时,群集可以在 四个小时内运行或还原.

下列哪种解决方案可以最好地以最具成本效益的方式最好地满足业务需求?

1. 确保已将 Amazon Redshift 集群设置为使用 Auto Scaling 组,并且集群中的节点分布在多个可用区中.
2. 确保使用 AWS CloudFormation 创建了 Amazon Redshift 集群模板,以便可以轻松地在另一个可用区中启动它,并从存储在 Amazon S3 中的自动 Redshift 备份中填充数据.
3. 使用 Amazon Kinesis Data Firehose 在摄取到 Amazon Redshift 之前收集数据,并使用另一个区域中的 AWS CloudFormation 创建集群并将数据流传输到两个集群.
4. 在不同区域中创建两个相同的 Amazon Redshift 集群(一个作为主集群,一个作为辅助集群).从主数据库到辅助数据库使用 Amazon S3 跨区域复制).用

Amazon S3 从主区域到辅助区域的跨区域复制,这会触发 AWS Lambda 函数以在辅助区域中填充集群.

答案: B

解释:

A. Redshift 集群是单个 AZ

https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-clusters.html#az-considerations B.最佳实践 C.我们有 4 小时的RPO,因此我们不需要冗余集群 D .没有意义,lambda 可能超时..

Question 32 **11/19考试原题**

一家公司倾向于将运行 Amazon EC2 实例的范围限制为从信息安全部门预先批准的 AMI 中启动的实例. 开发团队拥有敏捷的持续集成和部署过程,该解决方案无法阻止它.

哪种方法可以对开发过程产生最小的影响而执行所需的控制? (选择两个.)

1. 使用 IAM 策略来限制用户或其他自动化实体基于一组特定的预先批准的 AMI(例如由 Information Security 以特定方式标记的 AMI)启动 EC2 实例的能力.
2. 将 Amazon Inspector 中的常规扫描与自定义评估模板一起使用,以确定运行 Amazon Inspector 代理的

EC2 实例是否基于预先批准的 AMI.如果不是,请关闭实例,然后通过电子邮件通知安全信息.

1. 仅允许使用集中式 DevOps 团队启动 EC2 实例,该团队通过内部票务系统的通知获得工作包.用户使用此票证工具请求资源,该工具具有手动信息安全批准步骤,以确保仅从批准的 AMI 启动 EC2 实例.
2. 使用 AWS Config 规则发现基于未经批准的 AMI 的 EC2 实例的任何启动,触发 AWS Lambda 函数以自动终止实例,并将消息发布到 Amazon SNS 主题以通知 Information Security 发生了这种情况.
3. 使用预定的 AWS Lambda 函数扫描虚拟私有云(VPC)中正在运行的实例的列表,并确定其中是否基于未经批准的 AMI.将消息发布到 SNS 主题,以通知 Information Security 发生了这种情况,然后关闭实例.

答案: AD

解释:

B.AWS 检查器用于查找安全漏洞,不用于查找 AMI.C.不敏捷.E.计划的 lambda 不是问题,您需要

cloudwatch 事件来触发 Lambda

Question 33 **12/12考试原题**

某公司发生了安全事件,其中包含敏感信息的 Amazon S3 存储桶被公开.公司政策是永远不要有公共S3

对象,并且在发现任何公共对象时必须立即通知合规团队.

如何检测到公共 S3 对象的存在,将其设置为触发警报通知并在将来自动修复? (选择两个.)

1. 打开 Amazon S3 的对象级日志记录.启用具有公共读取权限的 PutObject API 调用时,请打开 Amazon S3 事件通知以使用 Amazon SNS 主题进行通知.
2. 配置一个 Amazon CloudWatch Events 规则,该规则调用一个 AWS Lambda 函数来保护 S3 存储桶.
3. 使用 AWS Trusted Advisor 的 S3 存储桶权限,并配置 CloudWatch 事件以使用 Amazon SNS 进行通知.
4. 打开 Amazon S3 的对象级日志记录.配置一个 CloudWatch 事件,以便在 AWS CloudTrail 日志中检测到具有公共读取权限的 PutObject API 调用时使用 SNS 主题进行通知.
5. 安排一个递归 Lambda 函数来定期更改 S3 存储桶中的所有对象权限.

答案: DE

解释:

A.S3 事件在某些情况下可能会丢失,并且可能需要几分钟才能到达https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html S3 事件消息不包含有关权限 https 的信息 B.不确定事件的来源是 C.我们可以向信任顾问提出建议,但可以使用信任策略顾问不会帮忙.

Question 34 **11/19考试原题 03/23考题**

一家公司正在使用 Amazon CloudFront 分发来分发来自在 Application Load Balancer 后面运行的 Web 应用程序的静态和动态内容. Web 应用程序需要用户授权和对动态内容的会话跟踪. CloudFront 分发具有配置为将授权,主机和用户代理 HTTP 白名单标头和会话 cookie 转发到源的单个缓存行为.所有其他缓存行为设置均设置为其默认值.

有效的 ACM 证书将在分配设置中使用匹配的 CNAME 应用于 CloudFront 分配. ACM 证书也应用于应用程序负载平衡器的 HTTPS 侦听器. CloudFront 原始协议策略设置为仅 HTTPS.对缓存统计信息报告的分析表明,此分布的未命中率很高.

解决方案架构师可以采取什么措施来提高此分发的缓存命中率,而又不会导致 CloudFront 与应用程序负载平衡器之间的 SSL / TLS 握手失败?

1. 为静态和动态内容创建两个缓存行为.如果发生缓存行为,请从白名单标头部分中删除 User-Agent 和Host HTTP 标头.从白名单 cookie 部分中删除会话 cookie,并从白名单标题部分中删除Authorization HTTP 标头,以配置为静态内容配置的缓存行为.
2. 从缓存行为的白名单头部分中删除 User-Agent 和 Authorization HTTPS 头.然后更新缓存行为,以使用预签名的 cookie 进行授权.
3. 从白名单标头部分删除 Host HTTP 标头,并从白名单 cookie 部分删除会话 cookie,以实现默认缓存行为.启用自动对象压缩,并将 Lambda @ Edge 查看器请求事件用于用户授权.
4. 为静态和动态内容创建两个缓存行为.从两种缓存行为的白名单标头部分中删除User-Agent HTTP 标头.从白名单 cookie 部分中删除会话 cookie,并从白名单标题部分中删除 Authorization HTTP 标头,以配置为静态内容配置的缓存行为.

答案: D

解释:

A.Host 标头需要传入,因为 CloudFront 和原始服务器使用相同的证书,这意味着证书的域列表可能与原始域名不匹配,然后需要 hHost 标头 https://docs.aws.amazon. com / AmazonCloudFront / latest / DeveloperGuide / http-502-bad-gateway.html B.静态内容在没有会话Cookie 的情况下效果更好

Question 35 **12/12考试原题 03/09考试原题**

一个组织拥有一个使用 Amazon API Gateway,AWS Lambda 和 Amazon DynamoDB 的写密集型移动应用程序.该应用程序已很好地扩展,但是,由于 Lambda 成本高于预期,因此成本成倍增加.该应用程序的使用无法预测,但是每月的使用率一直稳定增长 20%.

在监视当前的 Lambda 函数时,解决方案架构师注意到执行时间平均为 4.5 分钟.大多数等待时间是对本地 3TB MySQL 数据库服务器进行高延迟网络调用的结果. VPN 用于连接到 VPC,因此 Lambda 功能已配置为 5 分钟超时.

解决方案架构师如何降低当前架构的成本?

1. 将 VPN 替换为 AWS Direct Connect,以减少本地 MySQL 数据库的网络延迟. 在移动应用程序中启用本地缓存以减少 Lambda 函数调用.

监视 Lambda 函数性能；在保持可接受的执行时间的同时,逐渐将超时和内存属性调整为较低的值. 将频繁访问的记录从 DynamoDB 卸载到 Amazon ElastiCache.

1. 用 AWS Direct Connect 替换 VPN,以减少到本地 MySQL 数据库的网络延迟. 将 API 网关结果缓存到 Amazon CloudFront.

使用 Amazon EC2 预留实例代替Lambda.

在 EC2 上启用Auto Scaling,并在高峰时段使用竞价型实例.启用 DynamoDB Auto Scaling 来管理目标利用率.

1. 将 MySQL 数据库服务器迁移到 MySQL 的多可用区 Amazon RDS.

启用 Amazon API Gateway 的缓存会导致 Amazon CloudFront 减少 Lambda 函数调用的次数.

监视 Lambda 函数性能；在保持可接受的执行时间的同时,逐渐将超时和内存属性调整为较低的值. 为频繁访问的记录启用 DynamoDB Accelerator,并启用 DynamoDB Auto Scaling 功能.

1. 将 MySQL 数据库服务器迁移到 MySQL 的多可用区 Amazon RDS.

在 API Gateway 上启用 API 缓存以减少 Lambda 函数调用的次数.继续监视 AWS Lambda 函数性能； 在保持可接受的执行时间的同时,逐渐将超时和内存属性调整为较低的值.在 DynamoDB 中启用 Auto Scaling.

答案: D

解释:

A 如果延迟来自本地网络(即本地网络本身的超级慢),这将无济于事.B.EC2 较贵,直接连接也不便宜 C.随着应用程序扩展性好,我们可能不需要花费更多金钱的 DAX 和 Cloudfront.此外,如果使用 DAX,所有请求将首先发送到 DAX 群集.您不能只为某些记录启用 DAX.

Question 36

一家公司运行视频处理平台.文件由连接到 Web 服务器的用户上传,该服务器将文件存储在 Amazon EFS 共享上.该 Web 服务器在单个Amazon EC2 实例上运行.在 Auto Scaling 组中运行的一组不同的实例会扫描 EFS 共享目录结构,以查找要处理的新文件,并根据说明文件生成新的视频(缩略图,不同的分辨率,压缩等),该文件随同上传视频文件.在由 Auto Scaling 组管理的一组实例上运行的其他应用程序将处理视频文件,然后将其从 EFS 共享中删除.结果存储在 S3 存储桶中.指向已处理视频文件的链接将通过电子邮件发送给客户.

该公司最近发现,随着它们向 Auto Scaling Group 中添加更多实例,许多文件被处理了两次,因此图像处理速度没有得到改善.这些视频文件的最大大小为 2GB.

解决方案架构师应该怎么做才能提高可靠性并减少视频文件的冗余处理?

1. 修改 Web 应用程序以将视频文件直接上传到 Amazon S3.每次上传文件时,请使用 Amazon CloudWatch Events 触发 AWS Lambda 函数,并让此 Lambda 函数将消息放入新文件的 Amazon 队列中, 并使用队列深度指标来缩放视频处理 Auto Scaling 组中的实例.
2. 在 Web 服务器实例上设置 cron 作业,以将 EFS 共享的内容同步到 Amazon S3 中.每次上传文件以处理视频文件并将结果存储在 Amazon S3 中时,触发一次 AWS Lambda 函数.使用 Amazon CloudWatch Events 会触发 Amazon SES 作业,以将包含已处理文件链接的电子邮件发送给客户.
3. 重写 Web 应用程序以直接从 Amazon S3 运行,并使用Amazon API Gateway 将视频文件上传到 S3 存储桶.每次上载文件时,使用 S3 触发器运行 AWS Lambda 函数以在不同的存储桶中处理和存储新的视频文件.使用 CloudWatch Events,触发 SES 作业以向 cu 发送电子邮件
4. 重写 Web 应用程序以直接从 Amazon S3 运行,并使用Amazon API Gateway 将视频文件上传到 S3 存储桶.每次上载文件时,使用 S3 触发器运行 AWS Lambda 函数以在不同的存储桶中处理和存储新的视频文件.使用 CloudWatch Events,触发 SES 作业以向客户发送一封电子邮件,其中包含指向已处理文件的链接.
5. 重写要从 Amazon S3 运行的应用程序,并将视频文件上传到 S3 存储桶.每次上传新文件时,触发一个AWS Lambda 函数以将消息放入包含链接和说明的 SQS 队列中.修改视频处理应用程序以从 SQS 队列和 S3 存储桶中读取.使用队列深度度量标准来调整视频处理实例的 Auto Scaling 组的大小.

答案: D

解释:

A. Cloudwatch 事 件 不 支 持 s3 https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html B.Cloudwatch 事件不支持 s3 Lambda 具有并发限制 C.Lambda 具有 1000 个并发执行.如果每个上传尝试触发 lambda 来处理视频,则 D 无法正常工作.由于 lambda 执行具有并发限制,因此需要一个队列.视频

处理也可能需要很长时间,因为最大大小为 2GB. Lambda 具有 900s 的执行限制和 1000 个并发执行.对于 lambda,2GB 内存也很多.对于选项 A,S3 不支持 cloudwatch 事件,您将需要 cloudtrail https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/EventTypes.html

Question 37 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

解决方案架构师必须为大型的 Windows 和 Linux 服务器混合舰队制定补丁计划.补丁计划必须安全实施, 必须经过审核,并符合公司的业务要求.

通过最小的努力,哪个选项可以满足这些要求?

1. 安装并使用 OS 本地修补程序服务来管理所有实例的更新频率并发布批准.使用 AWS Config 来验证每个实例上的操作系统状态,并报告任何补丁程序合规性问题.
2. 在所有实例上使用 AWS Systems Manager 来管理修补程序.在生产之外测试补丁,然后在维护窗口中通过相应的批准进行部署.
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 OS 命令以获取并在每个实例上安装更新,包括在维护窗口期间进行的所有必需的重新启动.
4. 将所有应用程序迁移到 AWS OpsWorks,并使用 OpsWorks 自动修补支持以使 OS 在初始安装后保持最新状态.使用 AWS Config 提供审核和合规性报告.

答案: B

解释:

A. AWS Config 无法监视操作系统状态 C.对于 OpsWorks,建议的方法是替换旧实例,并且在安装过程中将应用安全更新

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/userguide/workingsecurity-updates.html

Question 38 **12/12考试原题 03/09考试原题**

解决方案架构师必须设计一个高可用性,无状态的 REST 服务.该服务将需要多个持久性存储层,以用于服务对象元信息和内容传递.每个请求都需要进行身份验证和安全处理.是否有要求保持尽可能低的成本?

如何满足这些要求?

1. 使用 AWS Fargate 托管运行自包含 REST 服务的容器.设置由应用程序负载平衡器(ALB)前置的Amazon ECS 服务.使用自定义身份验证器控制对 API 的访问.将请求元信息与 Auto Scaling 一起存储在Amazon DynamoDB 中,并将静态内容存储在安全的S3 存储桶中.发出对 Amazon S3 对象的安全签名请求,并通过 REST 服务接口代理数据.
2. 使用 AWS Fargate 托管运行自包含 REST 服务的容器.设置跨区域 ALB 前面的 ECS 服务.使用

Amazon Cognito 用户池来控制对 API 的访问.

将请求元信息与 Auto Scaling 一起存储在 DynamoDB 中,并将静态内容存储在受保护的 S3 存储桶中.返回对存储在 Amazon S3 中的内容的引用时,生成预签名 URL.

1. 设置 Amazon API Gateway 并创建所需的 API 资源和方法.使用

Amazon Cognito 用户池可控制对 API 的访问.配置方法以使用 AWS Lambda 代理集成,并使用唯一的

AWS Lambda 函数处理每个资源.

将请求元信息与 Auto Scaling 一起存储在 DynamoDB 中,并将静态内容存储在受保护的 S3 存储桶中.返回对存储在 Amazon S3 中的内容的引用时,生成预签名 URL.

1. 设置 Amazon API Gateway 并创建所需的 API 资源和方法.使用 Amazon API Gateway 定制授权者来控制对 API 的访问.配置方法以使用 AWS Lambda 自定义集成,并使用唯一的 Lambda 函数处理每个资源.将请求元信息存储在 Amazon ElastiCache 多可用区集群中,并将静态内容存储在受保护的 S3 存储桶中.

返回对存储在 Amazon S3 中的内容的引用时,生成预签名 URL.

答案: C

解释:

答.一个容器不是 HA,并且自定义身份验证器在 ECS 中不是问题(它在 API Gateway 中).虽然 Alb 支持cognito 或其他 IDP 授权,但这在答案中含糊不清.另外,使用签名的请求时,您无需代理 S3 内容. B.一个容器不是 HA,并且 Fargate 容器不会记录 API 调用日志,例如 API 网关.虽然 ALB 具有访问日志.总体而言, 此解决方案比 C D.昂贵.ElastiCache 不是持久性存储层. Lambda 自定义集成很难用于处理具有唯一功能的每个请求,因为您将需要使用 VTL 为不同的终结点定义映射.

Question 39 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

一家大型公司的每月 AWS 支出大幅增加.这是在开发人员在意外区域意外启动 Amazon EC2 实例之后. 该公司已针对开发人员的最低特权建立了实践,并使用Active Directory 组控制对本地资源的访问.该公司现在希望通过限制开发人员对 AWS 管理控制台的访问级别来控制成本,而又不影响其生产力.该公司还希望允许开发人员仅在一个区域中启动 Amazon EC2,而不限制对任何区域中其他服务的访问.

该公司如何在最小化运营团队的管理负担的同时达到这些新的安全要求?

1. 设置与附加了 AdministrativeAccess 托管策略的 IAM 角色绑定的基于 SAML 的身份验证.附加一个客户托管的策略,该策略拒绝访问每个区域中的 Amazon EC2(必需的策略除外).
2. 为每个开发人员创建一个 IAM 用户,并将它们添加到已附加 PowerUserAccess 托管策略的开发人员

IAM 组.附加客户托管的策略,该策略仅允许开发人员在所需区域中访问 Amazon EC2.

1. 设置与 IAM 角色绑定的基于 SAML 的身份验证,该角色具有 PowerUserAccess 托管策略和客户托管策略,这些策略拒绝所有开发人员访问除AWS Service Catalog 以外的任何 AWS 服务.在 AWS Service Catalog 中,创建一个仅包含批准区域中 EC2 资源的产品.
2. 设置与附加了 PowerUserAccess 托管策略的 IAM 角色绑定的基于 SAML 的身份验证.附加一个客户托管的策略,该策略拒绝访问每个区域中的 Amazon EC2(必需的策略除外).

答案: D

解释:

A.AdministrativeAccess 不是托管策略.如果我们谈论的是 AdministratorAccess,这将使开发人员有权更改 IAM 策略和角色,这不是理想选择,并且不能阻止他们更改拒绝策略以创建 EC2 B.IAM 评估检查至少允许是否存在拒绝.特定区域的 PowerUserAccess +允许不会停止其他区域的访问https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\_policies\_evaluation-logic.html#policy- eval-basicC.这将限制对其他区域的访问服务 C 无其他限制

Question 40

一家公司正在为在 AWS 上运行的应用程序确定其备份解决方案的体系结构.所有应用程序都在 AWS 上运行,并且在每个层中至少使用两个可用区.

公司政策要求 IT 部门将其所有数据的夜间备份持久地存储在至少两个位置:生产和灾难恢复.这些位置必须位于不同的地理区域.该公司还需要备份可立即在生产数据中心恢复,并在 24 小时内在灾难恢复位置恢复.所有备份过程必须完全自动化.

什么是可以满足所有要求的最具成本效益的备份解决方案?

1. 将所有数据备份到生产区域中附加到备份媒体服务器的大型 Amazon EBS 卷.运行自动化脚本以每晚对这些卷进行快照,然后将这些快照复制到灾难恢复区域.
2. 将所有数据备份到灾难恢复区域中的 Amazon S3.使用生命周期策略将这些数据立即移至生产区域中的 Amazon Glacier.仅复制数据；

从灾难恢复区域的 S3 存储桶中删除数据.

1. 将所有数据备份到生产区域中的 Amazon Glacier.将此数据跨区域复制到灾难恢复区域中的Amazon Glacier.设置生命周期策略以删除所有 60 天以上的数据.
2. 将所有数据备份到生产区域中的 Amazon S3.设置此S3 存储桶到另一个区域的跨区域复制,并在第二个区域中设置生命周期策略,以立即将该数据移至 Amazon Glacier.

答案: D

解释:

A.EBS 的价格大约是 S3 的 10 倍 B.冰川检索可能要花费数小时(虽然不是 S3 冰川)C.冰川检索可能要花费数小时

Question 41 **03/23考题**

公司拥有现有的本地三层 Web 应用程序. Linux Web 服务器从 NAS 服务器上的集中式文件共享中提供内容,因为每天都会从各种来源刷新几次内容.现有的基础架构尚未优化,该公司希望迁移到 AWS,以获得响应负载而上下扩展资源的能力.本地和AWS 资源使用 AWS Direct Connect 连接.

公司如何在不延迟内容刷新流程的情况下将 Web 基础架构迁移到 AWS?

1. 在 AWS 上的经典负载均衡器之后创建 Web 服务器 Amazon EC2 实例的集群.在内容的所有实例之间共享一个 Amazon EBS 卷.安排此卷和 NAS 服务器的定期同步.
2. 使用 AWS Storage Gateway 创建本地文件网关,以替换 NAS 服务器并将内容复制到 AWS.在 AWS 端, 将相同的 Storage Gateway 存储桶安装到每个 Web 服务器 Amazon EC2 实例以提供内容.
3. 将 Amazon EFS 共享公开给本地用户以充当NAS 服务.将相同的 EFS 共享装载到 Web 服务器

Amazon EC2 实例以提供内容.

1. 在 Auto Scaling 组中的 AWS 上创建 Web 服务器 Amazon EC2 实例.配置每晚从 NAS 服务器更新

Web 服务器实例的过程.

答案: C

解释:

A.EBS 卷可以 B.Storge 网关存储在 S3 中,并且无法跨实例共享,也不能正式安装 S3 存储桶. C.这很好,因为 EFS 是一种NAS,在这种情况下易于支持 D.刷新过程最多延迟 24 小时

Question 42 **12/12考试原题 03/09考试原题**

一家公司有多个托管 IT 应用程序的 AWS 账户. Amazon CloudWatch Logs 代理已安装在所有 Amazon EC2 实例上.该公司希望将所有安全事件汇总到专用于日志存储的集中式 AWS 账户中.

安全管理员需要跨多个 AWS 账户执行近乎实时的事件收集和关联. 哪种解决方案满足这些要求?

1. 在具有查看权限的每个应用程序 AWS 账户中创建日志审核 IAM 角色

CloudWatch Logs,配置 AWS Lambda 函数以承担日志审核角色,并每小时将 CloudWatch Logs 数据导出到日志记录 AWS 账户中的 Amazon S3 存储桶.

1. 在每个应用程序 AWS 帐户中配置 CloudWatch Logs 流,以将事件转发到日志记录 AWS 帐户中的CloudWatch Logs.在日志记录的 AWS 帐户中,将 Amazon Kinesis Data Firehose 流订阅到 Amazon CloudWatch Events,然后使用该流将日志数据持久存储在 Amazon S3 中.
2. 在日志帐户中创建 Amazon Kinesis Data Streams,将流订阅到

CloudWatch Logs 每个应用程序 AWS 账户中的流,使用数据流作为源配置 Amazon Kinesis Data Firehose 交付流,并将日志数据保留在日志记录 AWS 账户内的 Amazon S3 存储桶中.

1. 配置 CloudWatch Logs 代理以将数据发布到日志记录的 AWS 账户中的 Amazon Kinesis Data Firehose 流,使用 AWS Lambda 函数从流中读取消息并将消息推送到 Data Firehose,并将数据保留在Amazon S3 中.

答案: C

解释:

A.不是近实时 B.CloudWatch 事件不用于流日志,也不能用于流日志C.https://aws.amazon.com/blogs/architecture/central-logging-in-multi -account-environments / D.CloudWatch 代理无法将日志直接发送到 kinesis(也许我是错的)正式地,firehose 无法将数据流传输到lambda 函数,尽管您可以使用数据转换 lambda 来达到目的,但这是一种不好的做法.

Question 43

一家公司拥有由 Amazon CloudFront,Amazon API Gateway 和 AWS Lambda 函数组成的无服务器应用程序.应用程序代码的当前部署过程是创建 Lambda 函数的新版本号并运行 AWS CLI 脚本进行更新.如果新功能版本有错误,则另一个 CLI 脚本将通过部署该功能的先前工作版本来还原.该公司希望减少部署Lambda 函数提供的新版本的应用程序逻辑的时间,并希望减少发现错误后进行检测和还原的时间.

如何做到这一点?

1. 创建和部署嵌套的 AWS CloudFormation 堆栈,其父堆栈由 AWS CloudFront 发行版和 API 网关组成, 子堆栈包含 Lambda 函数.对于 Lambda 的更改,请创建一个 AWS CloudFormation 更改集并进行部署； 如果触发了错误,请将 AWS CloudFormation 更改集还原为先前版本.
2. 使用 AWS SAM 和内置的 AWS CodeDeploy 部署新的 Lambda 版本,将流量逐渐转移到新版本,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,则进行回滚.
3. 将 AWS CLI 脚本重构为部署新 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,请还原到以前的 Lambda 版本.
4. 创建并部署一个 AWS CloudFormation 堆栈,该堆栈由引用新 Lambda 版本的新 API Gateway 端点组成.将 CloudFront 来源更改为新的 API 网关终端节点,监视错误,如果检测到错误,则将 AWS CloudFront 来源更改为先前的 API 网关终端节点.

答案: B

解释:

A 可以将其用于回滚触发器.但是问题是 API 网关在更新或回滚时也需要更新以指向不同的 Lambda 版本B.最佳实践 C.需要将 api 网关更新为指向其他版本 D.不是自动进行的另外,可能无法使用具有相同 URL 的 API 网关端点

Question 44 **11/19考试原题 03/23考题**

一家公司正在 AWS 上运行.NET 三层 Web 应用程序.该团队目前使用 XL 存储优化实例来将网站的图片和视频文件存储在本地实例存储中.该公司遇到了由于复制和实例故障而导致数据丢失的问题.已要求解决方案架构师重新设计该应用程序,以提高其可靠性,同时保持较低的成本.

哪种解决方案可以满足这些要求?

1. 设置一个新的 Amazon EFS 共享,将所有图像和视频文件移动到该共享,然后将该新驱动器作为安装点附加到所有现有服务器.使用 Auto Scaling 通用实例创建 Elastic Load Balancer.对 Elastic Load Balancer 启用 Amazon CloudFront.启用 Cost Explorer 并使用AWS Trusted Advisor 检查继续监视环境以节省将来的费用.
2. 使用通用实例类型和 Elastic Load Balancer 实施 Auto Scaling.启用到 Amazon S3 的 Amazon CloudFront 分发,并将图像和视频文件移动到 Amazon S3.

保留通用实例以满足基本性能要求.使用 Cost Explorer 和 AWS Trusted Advisor 检查以继续监视环境以节省将来的费用.

1. 使用 S3 网站托管功能将整个网站移至 Amazon S3.删除所有 Web 服务器,并使 Amazon S3 与

Amazon VPC 中的应用程序服务器直接通信.

1. 使用 AWS Elastic Beanstalk 部署.NET 应用程序.将所有图像和视频文件移动到 Amazon EFS.创建一个指向 EFS 共享的 Amazon CloudFront 分配.保留满足基本性能要求所需的 m4.4xl 实例.

答案: B

解释:

A.S3 是使成本保持较低的更好的选择 C.S3 无法与其他服务进行通信.其他服务可以访问 S3.但是,对于这一应用程序,如果应用服务器没有 nat,我们将需要 VPC 端点 D.Cloudfront 无法直接指向 EFS

Question 45 **11/19考试原题**

一家公司开发了一个可在一个 AWS 区域中的 Amazon EC2 实例上运行的 Web 应用程序.该公司在其他国家/地区开展了新业务,必须将其应用程序部署到其他国家/地区,以满足其用户的低延迟要求.可以隔离区域,并且在一个区域中运行的应用程序不需要与其他区域中的实例进行通信.

公司的解决方案架构师应如何使应用程序部署自动化,以便可以将其最有效地部署到多个区域?

1. 编写一个 bash 脚本,该脚本使用 AWS CLI 在一个区域中查询当前状态并输出 JSON 表示形式.将

JSON 表示形式传递到 AWS CLI,并指定--region 参数以将应用程序部署到其他区域.

1. 编写一个 bash 脚本,该脚本使用 AWS CLI 在一个区域中查询当前状态并输出一个 AWS CloudFormation 模板.使用 AWS CLI 从模板创建 CloudFormation 堆栈,指定--region 参数以将应用程序部署到其他区域.
2. 在资源部分中编写一个 CloudFormation 模板来描述应用程序的基础结构.

使用 AWS CLI 从模板创建 CloudFormation 堆栈,使用--regions 参数指定多个区域以部署应用程序. D.在"资源"部分中编写一个 CloudFormation 模板来描述应用程序的基础结构.

使用管理员帐户中的 CloudFormation 堆栈集来启动将应用程序部署到其他区域的堆栈实例.

答案: D

解释:

C .-- region 存在,但是--regions 在 aws CLI 中不是问题

Question 46

一家媒体公司拥有 30 TB 的数字新闻视频存储库.这些视频存储在本地磁带库中的磁带上,并由媒体资产管理(MAM)系统引用.该公司希望以自动化的方式丰富这些视频的元数据,并通过使用 MAM 功能将其放入可搜索的目录中.公司必须能够基于视频中的信息进行搜索,例如物体,风景物品或人脸.提供了一个目录, 其中包含出现在视频中的人的面孔,其中包括每个人的图像.该公司希望将这些视频迁移到 AWS.

该公司与 AWS 建立了高速 AWS Direct Connect 连接,并希望将 MAM 解决方案视频内容直接从其当前文件系统中移出.

通过使用最少的持续管理开销并导致对现有系统的最小破坏,如何满足这些要求?

1. 在本地设置一个 AWS Storage Gateway 文件网关设备.使用 MAM 解决方案从当前存档中提取视频,并将其推送到文件网关中.使用面部目录在 Amazon Rekognition 中构建集合.构建一个 AWS Lambda 函数, 该函数调用 Rekognition Javascript SDK,以使 Rekognition 从支持文件网关的 Amazon S3 文件中提取视频,检索所需的元数据,然后将元数据推送到 MAM 解决方案中.
2. 在本地设置 AWS Storage Gateway,磁带网关设备.使用 MAM 解决方案从当前存档中提取视频并将其推送到磁带网关.使用面部目录在 Amazon Rekognition 中构建集合.构建一个 AWS Lambda 函数,该函数调用 Rekognition Javascript SDK,以使 Amazon Rekognition 处理磁带网关中的视频,检索所需的元数据, 然后将元数据推送到 MAM 解决方案中.
3. 使用 Amazon Kinesis Video Streams 配置视频摄取流.使用面部目录在 Amazon Rekognition 中构建集合.将视频从 MAM 解决方案流式传输到Kinesis Video Streams.配置 Amazon Rekognition 以处理流式视频.然后,使用流使用者来检索所需的元数据,并将元数据推送到 MAM 解决方案中.配置流以将视频存储在 Amazon S3 中.
4. 设置运行 OpenCV 库的 Amazon EC2 实例.将视频,图像和面部目录从一个本地库复制到此 EC2 实例上安装的 Amazon EBS 卷中.

处理视频以检索所需的元数据,然后将元数据推送到 MAM 解决方案中,同时还将视频文件复制到 Amazon S3 存储桶.

答案: A

解释:

B.Tape 将需要在某个地方还原才能访问.C.我不认为您可以配置视频流以将视频直接保存在 S3 中(即使视频流在后台使用 S3).您将需要一个消费者来这样做.另外,此解决方案需要管理视频流,这会带来很多开销,因为我们在这里实际上不需要实时处理. https://github.com/awslabs/amazon-kinesis-video-streams- producer-sdk-java/issues/22 D.EBS 的最大大小为 16TB

Question 47 **11/19考试原题 03/23考题**

一家公司正在计划迁移用于软件测试的多个实验室环境.各种各样的自定义工具用于管理每个实验室的测 试运行.实验室使用不可变的基础结构进行软件测试运行,并将结果存储在高度可用的 SQL 数据库集群中. 尽管完全重写自定义工具超出了迁移项目的范围,但该公司仍希望在迁移期间优化工作负载.

哪种应用程序迁移策略可以满足此要求?

A.重新主持B.重新平台

C.重构/重新架构D.退休

答 案 : B

Question 48 **12/12考试原题** **11/19考试原题 03/09考试原题**

公司正在实施多帐户策略；但是,管理团队对 DNS 之类的服务可能变得过于复杂表示担忧.该公司需要一种解决方案,以允许在不同帐户的虚拟私有云(VPC)之间共享私有 DNS.该公司将总共拥有约 50 个帐户.

哪种解决方案可以创建最低复杂的 DNS 架构并确保每个 VPC 都能解析所有 AWS 资源?

1. 在中央帐户中创建一个共享服务 VPC,并创建一个从共享服务 VPC 到其他帐户中每个 VPC 的 VPC 对等连接.在 Amazon Route 53 中,在共享服务 VPC 和域和子域的资源记录集中创建一个私有区域.以编程方式将其他 VPC 与托管区域相关联.
2. 在所有帐户中的 VPC 之间创建 VPC 对等连接.将每个 VPC 的 VPC 属性 enableDnsHostnames 和enableDnsSupport 设置为" true".为每个 VPC 创建一个 Amazon Route 53 专用区域.为域和子域创建资源记录集.以编程方式将每个 VPC 中的托管区域与其他 VPC 相关联.
3. 在中央帐户中创建共享服务 VPC.创建从其他帐户中的 VPC 到共享服务 VPC 的 VPC 对等连接.在共享服务 VPC 中使用域和子域的资源记录集创建 Amazon Route 53 私有托管区域.允许通过 VPC 对等连接的 UDP 和 TCP 端口 53.
4. 在每个 VPC 中,将 VPC 属性 enableDnsHostnames 和 enableDnsSupport 设置为" false".使用私有虚拟接口创建一个 AWS Direct Connect 连接.允许通过虚拟接口的 UDP 和 TCP 端口 53.使用本地 DNS 服务器解析 AWS 上每个 VPC 中的 IP 地址.

答案: A

解释:

A 请记住一件事:关联需要以编程方式完成,因为专用托管区域与我们尝试关联的 VPC 不在同一帐户中. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs- different-accounts.html https://docs.aws.amazon.com/Route53/latest/DeveloperGuide /hosted-zone- private-associate-vpcs.html B.enableDnsHostnames:用于确定具有公共 IP 的 VPC 中的资源是否获得公共主机名 enableDnsSupport:用于确定 VPC https://docs.aws 中是否支持 AWS DNS .amazon.com / vpc / latest / userguide / vpc-dns.html 这实际上可以工作,但实际上不是必需的,因为您将要管理 50 个托管区域,并且需要配置 50 \* 49 VPC 对等.但是,每个 VPC 将具有不同的 Route 53 区域,这不共享 DNSC. 由于 VPC 对等不会阻塞任何内容,因此您实际上不需要允许端口 53,这是 NACL 的工作.但是,必须将Route 53 托管区域与 VPC 关联才能工作 D.这可以立即排除,因为直接连接用于本地到 AWS 连接

Question 49 **12/12考试原题 03/09考试原题**

一家公司发布了新版本的网站,以面向亚洲和南方的受众

美国.该网站的媒体资产托管在 Amazon S3 上并拥有一个 Amazon

CloudFront 分发可改善最终用户的性能.但是,用户的登录体验很差,身份验证服务仅在 us-east-1 AWS 区域中可用.

解决方案架构师如何以最小的管理开销改善登录体验并保持高安全性和性能?

1. 在每个新地理区域中复制设置,并使用基于 Amazon Route 53 的地理位置路由来将流量路由到离用户最近的 AWS 区域.
2. 使用 Amazon Route 53 加权路由策略将流量路由到CloudFront 分配.使用 CloudFront 缓存的 HTTP

方法来改善用户登录体验.

1. 使用附加到 CloudFront 查看器请求触发器的 Amazon Lambda @ Edge,通过维护会话期满的安全cookie 令牌来认证和授权用户,以改善多个地区的用户体验.
2. 复制每个地理位置的设置,并使用网络负载平衡器将流量路由到在与用户最近的区域中运行的身份验证 服务.

答案: C

解释:

A.太多的开销. B.无法缓存登录C.https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-generating-http- response-in-requests.html D.开销!!网络负载平衡器无法执行此操作

Question 50 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

公司具有使用两个可用区的标准三层体系结构.在公司淡季期间,用户报告该网站无法正常工作.解决方案架构师发现最近对环境没有任何更改,可以访问该网站,并且可以登录.但是,当解决方案架构师选择"在您附近找到商店"功能时,地图上提供的地图刷新页面后,通过第三方 RESTful API 调用的网站无法正常工作. 通过 Amazon EC2 NAT 实例进行出站API 调用.

造成此故障的最可能原因是什么?将来如何缓解?

A.一个子网的网络 ACL 阻止出站 Web 通信.打开网络 ACL,并防止管理员将来通过 IAM 进行更改. B.故障是在第三方环境中.请与提供地图的第三方联系,并请求修复程序以延长正常运行时间.

1. 一个 NAT 实例已经过载.将两个 EC2 NAT 实例替换为较大的实例,并确保在增加新实例大小时考虑到增长.
2. NAT 实例之一失败.建议使用 NAT 网关替换 EC2 NAT 实例.

答案: D

解释:

A 不能,因为有 50%的呼叫成功.C.可以工作,但实际上不是扩展性的好解决方案

Question 51 **03/23考题**

一家公司正在迁移到云.它希望评估其现有数据中心环境中虚拟机的配置,以确保其可以准确调整新Amazon EC2 实例的大小.该公司想要收集指标,例如 CPU,内存和磁盘利用率,并且需要清点每个实例上正在运行的进程.该公司还希望监视网络连接以映射服务器之间的通信.

哪个可以使该数据收集成本最低?

1. 使用 AWS Application Discovery Service 并将数据收集代理部署到数据中心中的每个虚拟机.
2. 在本地环境中的所有服务器上配置 Amazon CloudWatch 代理,并将指标发布到 Amazon CloudWatch Logs.
3. 使用 AWS Application Discovery Service 并在现有虚拟化环境中启用无代理发现.
4. 在 AWS 管理控制台中启用 AWS Application Discovery 服务,并将公司防火墙配置为允许通过 VPN 进行扫描.

答案: A

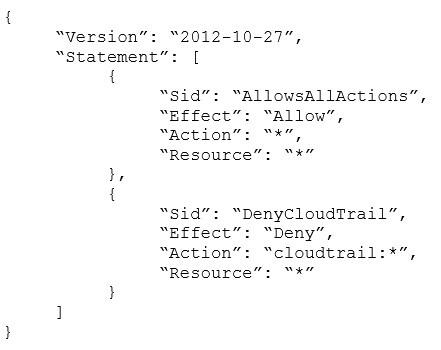
解释:

B.CloudWatch 代理用于发送日志项目,并且不监视网络流量 C.Agentless 发现无法获取流程信息

https://aws.amazon.com/application-discovery/faqs/#

Question 52

一个公司将有几个 AWS 账户正在使用 AWS 组织和服务控制策略(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(OU):



使用账户 1111-1111-1111 的开发人员抱怨他们无法创建 Amazon S3 存储桶. 管理员应如何解决此问题?

1. 向 SCP 添加"允许"效果的 s3:CreateBucket.
2. 从 OU 中删除帐户,并将 SCP 直接附加到帐户 1111-1111-1111.
3. 指示开发人员向其 IAM 实体添加 Amazon S3 权限.

D.从帐户 1111-1111-1111 中删除 SCP.

答案: C

解释:

A.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.仍将停止操作 C.IAM 无法覆盖 SCP,两者都需要允许该操作,但政策确实不要拒绝创建 s3 存储桶权限

D.会工作,可能不是最好的选择应该在某处写一个 SCP,但是 B,C 和 D 看起来根本不正确. https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\_policies\_evaluation-logic.html

Question 53 **12/12考试原题 03/09考试原题**

提供无线服务的公司需要一种解决方案来存储和分析有关用户活动的日志文件.当前,日志文件每天交付到 Amazon EC2 实例上的 Amazon Linux.批处理脚本每天运行一次,以汇总用于第三方工具分析的数据. 推送到第三方工具的数据用于为最终用户生成可视化效果.批处理脚本的维护很麻烦,并且需要花费数小时才能将不断增长的数据量交付给第三方工具.该公司希望降低成本,并愿意考虑使用一种新工具,以最大程度地减少开发工作并降低管理开销.该公司希望构建一个更加敏捷的解决方案,以最小的开销几乎实时地存储和执行分析.该解决方案必须具有成本效益和可扩展性,以满足公司最终用户群的增长.

哪种解决方案符合公司的要求?

1. 开发一个 Python 脚本以实时使 Amazon EC2 中的数据失效,并将数据存储在 Amazon S3 中.使用复制命令将数据从 Amazon S3 复制到 Amazon Redshift.将在 Amazon EC2 上运行的商业智能工具连接到Amazon Redshift 并创建可视化.
2. 使用在 Auto Scaling 组的 EC2 实例上运行的 Amazon Kinesis 代理收集数据并将其发送到 Amazon Kinesis Data Firehose 交付流. Kinesis Data Firehose 交付流将直接将数据交付给 Amazon ES.使用Kibana 可视化数据.
3. 使用在 Amazon EBS 优化的 EC2 实例上运行的内存缓存应用程序来近乎实时地捕获日志数据.在同一EC2 实例上安装 Amazon ES 集群,以存储日志文件,这些日志文件几乎实时地传递到 Amazon EC2.安装Kibana 插件以创建可视化.
4. 使用在 EC2 实例上运行的Amazon Kinesis 代理收集数据并将其发送到 Amazon Kinesis Data Firehose 交付流. Kinesis Data Firehose 交付流会将数据交付给 Amazon S3.使用 AWS Lambda 函数将数据从 Amazon S3 传递到 Amazon ES.使用 Kibana 可视化数据.

答案: B

解释:

72 A.Python 脚本将成为维护 C.2 的 EC2 太多的难点,非常昂贵的 D.Firehose 可以直接传递给 ES https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-aws-integrations.html

Question 54

一家公司希望将 Web 应用程序移至 AWS.该应用程序将会话信息本地存储在每个 Web 服务器上,这将使自动扩展变得困难.作为迁移的一部分,将重写应用程序以将会话数据与 Web 服务器分离.该公司要求低延迟,可伸缩性和可用性.

哪种服务将符合以最具成本效益的方式存储会话信息的要求? A.具有 Memcached 引擎的 Amazon ElastiCache

1. 亚马逊 S3
2. Amazon RDS MySQL
3. 带有 Redis 引擎的 Amazon ElastiCache

答案: D

解释:

Memcached 不是真正的 HA(无复制)

https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/SelectEngine.html

Question 55 **12/12考试原题 03/09考试原题**

一家公司的 Amazon EC2 部署具有以下架构:

-包含 8 个 m4.xlarge 实例的应用程序层

-经典的负载均衡器

-Amazon S3 作为持久数据存储

在其中一个 EC2 实例失败后,用户报告其请求的处理非常缓慢.

解决方案架构师必须建议设计更改,以最大程度地提高系统可靠性.该解决方案必须将成本降至最低. 解决方案架构师应该建议什么?

1. 使用 AWS Lambda 函数将现有 EC2 实例迁移到无服务器部署
2. 将经典负载均衡器更改为应用程序负载均衡器
3. 在 Auto Scaling 组中将应用程序层替换为 m4.large 实例
4. 用 4 个 m4.2xlarge 实例替换应用程序层答案: C

Question 56 **12/12考试原题**

本地应用程序将迁移到云中.该应用程序由一个 Elasticsearch 虚拟机和一个来自本地系统的数据源提要

(将不会迁移)以及一个运行在三个虚拟机上的 Apache Tomcat 上的 Java Web 应用程序组成. Elasticsearch 服务器当前使用 16 TB 可用存储中的 1 TB 存储,并且 Web 应用程序每 4 个月更新一次.多个用户从 Internet 访问 Web 应用程序.已建立 10Gbit AWS Direct Connect 连接,可以在计划的 48 小时更改窗口内迁移应用程序.

迁移后,哪种策略对运营人员的影响最小?

1. 在具有 2 TB 的 Amazon EBS 和适用于 Web 应用程序的公共 AWS Elastic Beanstalk 环境的大小合适的 Amazon EC2 上创建 Elasticsearch 服务器.暂停数据源,从本地导出 Elasticsearch 索引,然后导入 EC2 Elasticsearch 服务器.将数据源提要移动到新的 Elasticsearch 服务器,并将用户移动到 Web 应用程序.
2. 为 Elasticsearch 创建 Amazon ES 集群,为 Web 应用程序创建公共 AWS Elastic Beanstalk 环境.使用AWS DMS 复制 Elasticsearch 数据.复制完成后,将数据源提要移动到新的 Amazon ES 集群终端节点,并将用户移动到新的 Web 应用程序.
3. 使用 AWS SMS 将虚拟机复制到 AWS 中.迁移完成后,暂停数据源提要并启动已迁移的 Elasticsearch 和 Web 应用程序实例.将 Web 应用程序实例放置在公共 Elastic Load Balancer 后面.将数据源提要移动到新的 Elasticsearch 服务器,并将用户移动到新的 Web 应用程序负载均衡器.
4. 为 Elasticsearch 创建 Amazon ES 集群,为 Web 应用程序创建公共 AWS Elastic Beanstalk 环境.暂停数据源提要,从本地导出 Elasticsearch 索引,然后导入到 Amazon ES 集群中.将数据源提要移至新的Amazon ES 集群终端节点,并将用户移至新的 Web 应用程序.

答案: D

解释:

B. ES 不能成为 DMS 的来源

https://docs.aws.amazon.com/dms/latest/userguide/CHAP\_Source.html D.通过导入和导出,我认为这意味着快照和还原,否则在 ElasticSearch 中不会导出或导入索引.如果是这样,这是最好的答案,否则 C 将是唯一可行的解 决方案...

Question 57 **12/12考试原题 03/09考试原题**

由于数据库服务器上的大量读取,公司的应用程序越来越受欢迎,并且出现了延迟. 该服务具有以下属性:

-使用应用程序将高可用性 REST API 托管在一个区域中具有自动缩放功能的负载均衡器(ALB).

-单个托管在 Amazon EC2 实例上的 MySQL 数据库可用区.

-该公司希望减少延迟,提高区域内数据库的读取性能,并拥有可自动执行实时恢复而不会造成任何数据或 性能损失(HA / DR)的多区域灾难恢复功能.

哪种部署策略可以满足这些要求?

1. 使用 AWS CloudFormation StackSets 在两个区域中部署 API 层.将数据库迁移到具有 MySQL 数据库集群的 Amazon Aurora,该集群在一个区域中具有多个只读副本,在与源数据库集群不同的区域中具有一个只读副本.如果对主负载均衡器的运行状况检查失败,请使用 Amazon Route 53 运行状况检查触发DNS 故障转移到备用区域.如果发生 Route 53 故障转移,则将跨区域数据库副本提升为主数据库,并在备用区域中构建新的只读副本.
2. 使用具有自动故障转移功能的 Amazon ElastiCache for Redis Multi-AZ 来缓存数据库读取查询.使用AWS OpsWorks 在两个区域中部署 API 层,缓存层和现有数据库层.如果发生故障,请在数据库上使用Amazon Route 53 运行状况检查,如果主要区域中的运行状况检查失败,则触发 DNS 故障转移到备用区域.经常备份 MySQL 数据库,如果活动区域发生故障,请将备份复制到备用区域并还原备用数据库.
3. 使用 AWS CloudFormation StackSets 在两个区域中部署 API 层.将数据库添加到 Auto Scaling 组.将只读副本添加到第二个区域中的数据库.在主要区域中使用 Amazon Route 53 运行状况检查失败.提升跨区域数据库副本为主服务器,并在备用区域中构建新的只读副本.
4. 将 Amazon ElastiCache 与 Redis Multi-AZ 一起使用,具有自动故障转移功能来缓存数据库读取查询. 使用 AWS OpsWorks 在两个区域中部署 API 层,缓存层和现有数据库层.如果主要区域中的运行状况检查失败,请在 ALB 上使用 Amazon Route 53 运行状况检查触发 DNS 故障转移到备用区域.经常备份MySQL 数据库,如果活动区域发生故障,请将备份复制到备用区域并还原备用数据库.

答案: A

解释:

A.Aurora 群集默认为多可用区,这是最佳选择 B.无法进行活动故障转移 DB C.跨 EC2 共享数据量将是痛苦的 D.与 B 相同

Question 58 **12/12考试原题**

一家公司在 AWS 中运行三层应用程序.用户报告说,应用程序性能可能会因一天中的时间和所访问的功能而有很大差异.

该应用程序包括以下组件:

-八个 t2.large 前端 Web 服务器,它们提供来自应用程序层的静态内容和代理动态内容.

-四台 t2.large 应用程序服务器. -一个 db.m4.large Amazon RDS MySQL 多可用区数据库实例. 操作已确定 Web 层和应用程序层受网络限制.

以下哪项应能经济有效地提高应用程序性能? (选择两个.)

1. 用 t2.xlarge 实例替换 Web 和应用程序层
2. 将 AWS Auto Scaling 和 m4.large 实例用于 Web 和应用程序层
3. 将 MySQL RDS 实例转换为 Amazon EC2 上的自我管理MySQL 集群
4. 创建一个 Amazon CloudFront 发行版以缓存内容
5. 将 Amazon RDS 实例的大小增加到 db.m4.xlarge

答案: BD

解释:

由于约束是网络,因此 t2.xlarge 具有与m4.large 相同的网络性能,但价格更

高.https://aws.amazon.com/ec2/pricing/on-demand/ https://aws.amazon.com/ ec2 / instance-types /

Question 59 **11/19考试原题 03/23考题**

在线零售商需要定期处理大型产品目录,这些产品目录是分批处理的.这些已发送出去,供人们使用Amazon Mechanical Turk 服务进行处理,但零售商已要求其解决方案架构师设计工作流程编排系统,以使其能够处理多个并发的 Mechanical Turk 操作,处理结果评估流程并进行重新处理失败.

下列哪个选项使零售商能够以最少的实施工作量来询问每个工作流的状态?

1. 根据多个 Amazon SQS 队列(每个工作流程阶段一个队列)中的消息可见性触发 Amazon CloudWatch 警报,并通过Amazon SNS 发送消息以触发 AWS Lambda 函数以处理下一步.使用 Amazon ES 和Kibana 可视化 Lambda 处理日志以查看工作流程状态.
2. 使用 AWS Lambda 函数轮询 RDS 以获取状态更改,将工作流信息保存在 Amazon RDS 实例中.然后,Worker Lambda 函数将处理下一个工作流程步骤. Amazon QuickSight 将直接在 Amazon RDS 之外可视化工作流程状态.
3. 在 AWS Step Functions 中构建工作流程,使用它来编排多个并发工作流程.可以在 AWS 管理控制台中可视化每个工作流程的状态,并且可以将历史数据写入 Amazon S3 并使用Amazon QuickSight 可视化. D.使用 Amazon SWF 创建工作流,该工作流处理具有多个工作人员任务的单批目录记录,以提取数据,转换数据并通过 Mechanical Turk 发送数据.使用 Amazon ES 和 Kibana 可视化AWS Lambda 处理日志以查看工作流程状态.

答案: D

解释:

C.Step Function 在人工干预下可能无法很好地工作,并且我认为历史数据无法轻松地传递到 S3D.工作流最好由 SWF 或 Step Function 处理,因此将 A 和 B 排除在外.由于我们使用的是 Mechanical Turk HIT,因此需要人工干预(即访问成功的结果).在 https://aws.amazon.com/swf/faqs/中,SWF 也有一个类似的用例.

Question 60

一个组织有两个 Amazon EC2 实例:

-首先是运行订购应用程序和库存应用程序. -第二个运行排队系统.

在一年中的某些时候,每秒下达数千个订单.排队系统关闭时,一些订单丢失了.同样,组织的库存应用程序 具有错误的产品数量,因为某些订单已处理两次.

如何确保应用程序可以处理越来越多的订单?

1. 将订购和库存应用程序放入其自己的 AWS Lambda 函数中.让订购应用程序将消息写入 Amazon SQS FIFO 队列.
2. 将订购和库存应用程序放入其自己的 Amazon ECS 容器中,并为每个应用程序创建一个Auto Scaling

组.然后,在多个可用区域中部署消息队列服务器.

1. 将订购和库存应用程序放入其自己的 Amazon EC2 实例,并为每个应用程序创建一个Auto Scaling 组. 对接收的订单使用 Amazon SQS 标准队列,并在库存应用程序中实现幂等.
2. 将订购和库存应用程序放入其自己的 Amazon EC2 实例中.将传入订单写入 Amazon Kinesis 数据流中. 配置 AWS Lambda 以轮询流并更新清单应用程序.

答案: C

解释:

A.这看似不错的解决方案,但实际上无法使用,因为 Lambda 的并发限制为 1000,而我们需要每秒处理数千个订单. (尽管我们可以联系 AWS 来增加限额,但是对于考试而言,这并不是一个很好的答案). B.分布式排队系统在某个时候可能会有重复的消息.另外,自动缩放组在 ECS 中也不是问题(尽管是为 EC2 提供支持的 EC2)D.Kinesis 流没有消息级别的确认/失败,仍然会有重复或未处理的项目

Question 61 **12/12考试原题** **11/19考试原题 03/09考试原题**

一家公司正在将其本地构建工件服务器迁移到 AWS 解决方案.当前系统由 Apache HTTP 服务器组成,该服务器为外围网络限制的本地站点上的客户端提供构件.工件使用者主要是构建自动化脚本,这些脚本通过匿名 HTTP 下载工件,该公司将无法在其迁移时间表内对其进行修改.

该公司决定将解决方案移至 Amazon S3 静态网站托管.工件使用者将被迁移到虚拟私有云(VPC)中位于公共子网和私有子网内的 Amazon EC2 实例.

哪种解决方案将允许工件使用者在不修改现有自动化脚本的情况下下载工件?

1. 在 VPC 的公共子网中创建 NAT 网关.添加指向 NAT 的默认路由

网关进入与包含使用者的子网关联的路由表.配置条件策略以允许 s3:ListBucket 和 s3:GetObject 操作使用条件 IpAddress 和条件密钥 aws:SourceIp 与 NAT 网关匹配的弹性 IP 地址.

1. 创建一个 VPC 端点并将其添加到与包含以下内容的子网关联的路由表中

消费者.使用条件以及与 VPC StringEquals 端点的标识匹配的条件键 aws:sourceVpce,配置存储桶策略以允许 s3:ListBucket 和 s3:GetObject 操作.

1. 为 Amazon EC2 创建 IAM 角色和实例配置文件,并将其附加到使用构建工件的实例.配置存储桶策略, 以允许与创建的 IAM 角色匹配的主体使用 s3:ListBucket 和 s3:GetObjects 操作.
2. 创建一个 VPC 端点并将其添加到与包含使用者的子网关联的路由表中.

使用条件和与 VPC CIDR 块匹配的条件键 aws:SourceIp,配置存储桶策略以允许 s3:ListBucket 和

s3:GetObject 操作.

答案: B

解释:

A.这将通过公共互联网,显然不是最佳选择 C.专用子网中的实例无法访问存储桶 D.对于具有 VPC 端点的S3,您不能将 Sourceip 与 VPC CIDR 块一起使用 https://docs.aws.amazon .com / vpc / latest / userguide / vpc-endpoints-s3.html

Question 62 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

一组研究机构和医院正在合作研究 2 PB 的基因组数据.拥有数据的研究所将其存储在 Amazon S3 存储桶中并定期更新.该研究所希望授予合作伙伴关系中的所有组织对数据的读取权限.伙伴关系的所有成员都非常注重成本,并且拥有 S3 存储桶帐户的机构担心要支付来自 Amazon S3 的请求和数据传输的费用.

哪种解决方案可以确保安全的数据共享,而又不会导致拥有该存储桶的机构承担 S3 请求和数据传输的所有费用?

1. 确保合作伙伴关系中的所有组织都有 AWS 账户.在具有 S3 存储桶的帐户中,为合作伙伴关系中的每个帐户创建一个跨帐户角色,以允许对数据进行读取访问.

让组织在访问数据时承担并使用该读取角色.

1. 确保合作伙伴关系中的所有组织都有 AWS 账户.在拥有数据的存储桶上创建存储桶策略.该策略应允许合作伙伴关系中的帐户对存储桶进行读取访问.在水桶上启用请求者付款.让组织在访问数据时使用其AWS 凭证.
2. 确保合作伙伴关系中的所有组织都有 AWS 账户.使用存储区策略在每个帐户中配置存储区,该策略使拥有数据的机构可以写入存储区.定期将研究所帐户中的数据同步到其他组织.让组织在使用其帐户访问数据时使用其 AWS 凭证.
3. 确保合作伙伴关系中的所有组织都有 AWS 账户.在具有 S3 存储桶的帐户中,为合作伙伴关系中的每个帐户创建一个跨帐户角色,以允许对

数据.

在水桶上启用请求者付款.让组织在访问数据时承担并使用该读取角色.

答案: B

解释:

A.拥有数据的组织将支付所有费用 C.这将导致双重收费:写入和读取 D.拥有假定角色的账户将由请求者支 付 ..https://docs.aws.amazon.com /AmazonS3/latest/dev/RequesterPaysBuckets.html https://amazonaws-china.com/cn/premiumsupport/knowledge-center/s3-cross-account-a ccess-denied

/

Question 63 **12/12考试原题**

一家公司目前使用单个 1 Gbps AWS Direct Connect 连接来建立 AWS 区域与其数据中心之间的连接.该公司有五个 Amazon VPC,所有这些 VPC 都使用相同的Direct Connect 连接连接到数据中心.网络团队担心单点故障,并且对改善与 AWS 的连接的冗余性同时将成本保持在最低水平感兴趣.

哪种解决方案可以在满足成本要求的同时提高与 AWS 的连接的冗余性?

1. 设置另一个 1 Gbps Direct Connect 连接,并为每个 VPC 创建新的 VIF.使用 BGP 以负载平衡方式配置

VIF.

1. 设置从数据中心到每个 VPC 的 VPN 隧道.在相应 VPC 的虚拟专用网关(VGW)处终止每个 VPN 隧道, 并设置 BGP 进行路由管理.
2. 建立与正在使用的 AWS 区域的新的点对点多协议标签交换(MPLS)连接.将 BGP 配置为将此新电路用作被动电路,以便除非 AWS Direct Connect 失败,否则不会有流量通过此电路.
3. 在 Direct Connect 连接上创建一个公共VIF,并设置一个 VPN 隧道,该隧道将使用公共 VIF 在相应 VPC

的虚拟专用网关(VGW)上终止.使用 BGP 处理故障转移到 VPN 连接.

答案: B

解释:

A.VIF 不是 VGW,它与直接连接相关联 https://aws.amazon.com/premiumsupport/knowledge- center/public-private-interface-dx/ C.MPLS 仍通过直接连接 https://aws .amazon.com / answers / networking / aws-network-connectivity-over-mpls /D.不需要公共 VIF,除非您需要连接到 AWS 公共服务, 并且不需要公共 VIF 进行 VPN 连接

Question 64 **12/12考试原题** **11/19考试原题 03/23考题**

一家公司当前将 Amazon EBS 和 Amazon RDS 用于存储目的.该公司打算在不同的 AWS 区域中使用指示灯的方法进行灾难恢复.该公司的 RTO 为 6 小时,RPO 为 24 小时.

哪种解决方案可以以最低的成本达到要求?

1. 使用 AWS Lambda 创建每日 EBS 和 RDS 快照,并将它们复制到灾难恢复区域.将 Amazon Route 53 与主动-被动故障转移配置一起使用.在灾难恢复区域的容量设置为 0 的 Auto Scaling 组中使用 Amazon EC2.
2. 使用 AWS Lambda 创建每日 EBS 和 RDS 快照,并将它们复制到灾难恢复区域.将 Amazon Route 53 与主动-主动故障转移配置一起使用.在以与主要区域相同的方式配置的 Auto Scaling 组中使用 Amazon EC2.
3. 使用 Amazon ECS 处理长期运行的任务,以创建每日 EBS 和 RDS 快照,并将其复制到灾难恢复区域. 将 Amazon Route 53 与主动-被动故障转移配置一起使用.在灾难恢复区域的容量设置为 0 的 Auto Scaling 组中使用 Amazon EC2.
4. 使用 EBS 和 RDS 跨区域快照复制功能在灾难恢复区域中创建快照.将 Amazon Route 53 与主动-主动故障转移配置一起使用.在灾难恢复区域的容量设置为 0 的 Auto Scaling 组中使用 Amazon EC2.

答案: D

解释:

A.Lambda 不应用于快照 B.'EC2 配置相同方式'将是多站点 D.使用内置的跨区域复制将是最佳解决方案,

但 EBS 无法自动拍摄快照,您将需要 AWS 数据生命周期

Question 65

公司需要经济有效地保留小数据记录(最多 1 KiB)最多 30 天.很少读取数据.读取数据时,可以接受 5 分钟的延迟.

下列哪个解决方案可以实现此目标? (选择两个.)

1. 使用 Amazon S3 在一个 S3 对象中收集多个记录.写入后立即使用生命周期配置将数据移至Amazon Glacier.读取数据时,请使用快速检索.
2. 将记录写入 Amazon Kinesis Data Firehose 并配置 Kinesis Data Firehose 在 5 分钟后将数据传递到

Amazon S3.在 30 天的 S3 存储桶上设置到期操作.

1. 使用通过 Amazon API Gateway 调用的 AWS Lambda 函数收集数据 5 分钟.在 Lambda 执行停止之前, 将数据写入 Amazon S3.
2. 将记录写入配置了 30 天的生存时间(TTL)的 Amazon DynamoDB.使用 GetItem 或 BatchGetItem 调用读取数据.
3. 将记录写入 Redis 的 Amazon ElastiCache.配置 Redis 仅附加文件(AOF)持久性日志以写入 Amazon S3.如果 ElastiCache 实例失败,则从日志中恢复.

答案: AD

A.冰川检索可能长达 1-5 分钟,并且 Glacier 的最小大小收费为 40KB,但是最小存储时间为 90 天,即使它仍然比标准 S3 https://docs.aws 便宜得多.amazon.com / amazonglacier / latest / dev / downloading- an-archive-two-steps.html https://aws.amazon.com/s3/storage-classes/ BI 认为这意味着此处的消防水

带缓冲间隔.费用昂贵,因为每条记录会四舍五入到最接近的 5 KB 收费,因为记录全为 1 KB,在这种情况下, 我 们 可 以 多 支 付 5 倍 的 费 率 . https://docs.aws.amazon.com/firehose/latest/dev/basic- deliver.html#frequencyC.这并不是真正可靠的解决方案,因为我们长期运行 lambda,这不是 lambda 打算做 的 . 这 将 是 非 常 昂 贵 的 . API 网 关 也 会 在 30 秒 后 超 时 . 不 支 持 D.AOF 写 入 s3 https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/RedisAOF.html

Question 66

开发团队正在将新的 API 部署为公司内的无服务器应用程序.该团队当前正在使用AWS 管理控制台来供应 Amazon API Gateway,AWS Lambda 和 Amazon DynamoDB 资源.解决方案架构师的任务是自动化这些无服务器 API 的未来部署.

如何做到这一点?

1. 将 AWS CloudFormation 与 Lambda 支持的自定义资源一起使用以供应 API 网关.使用 AWS :: DynamoDB :: Table 和 AWS :: Lambda :: Function 资源创建 Amazon DynamoDB 表和 Lambda 函数.编写脚本以自动化 CloudFormation 模板的部署.
2. 使用 AWS 无服务器应用程序模型来定义资源.将 YAML 模板和应用程序文件上传到代码存储库.使用AWS CodePipeline 连接到代码存储库并创建要使用 AWS CodeBuild 进行构建的操作.使用CodePipeline 中的 AWS CloudFormation 部署提供程序来部署解决方案.
3. 使用 AWS CloudFormation 定义无服务器应用程序.在 Lambda 函数上实现版本控制,并创建别名以指向版本.部署时,配置权重以实现将流量转移到最新版本,并随着流量的移动逐渐更新权重.
4. 将应用程序代码提交到 AWS CodeCommit 代码存储库.使用 AWS CodePipeline 并连接到CodeCommit 代码存储库.使用 AWS CodeBuild 通过 AWS CodeDeploy 构建和部署 Lambda 函数.在CodeDeploy 中指定部署首选项类型,以将流量逐渐转移到新版本.

答案: B

解释:

A.API 网关 cloudformation 受支持,不需要自定义资源 B.SAM 部署只是 cloudformation 部署的别名

https://docs.aws.amazon.com/serverless-application-model/latest/developer

Question 67

公司安全团队查询所有上传到 Amazon S3 存储桶的数据都必须加密.加密密钥必须具有高可用性,并且公司必须能够基于每个用户控制访问,并且不同的用户可以访问不同的加密密钥.

以下哪种架构可以满足这些要求? (选择两个.)

1. 将 Amazon S3 服务器端加密与 Amazon S3 托管密钥一起使用.允许 Amazon S3 生成 AWS / S3 主密钥,并使用 IAM 控制对生成的数据密钥的访问.
2. 将 Amazon S3 服务器端加密与 AWS KMS 托管密钥一起使用,创建多个客户主密钥,并使用密钥策略来控制对其的访问.
3. 将 Amazon S3 服务器端加密与客户管理的密钥一起使用,并使用AWS CloudHSM 来管理密钥.使用

CloudHSM 客户端软件来控制对生成的密钥的访问.

1. 将 Amazon S3 服务器端加密与客户管理的密钥一起使用,并使用在高可用性模式下配置的两个 AWS CloudHSM 实例来管理密钥.使用 Cloud HSM 客户端软件来控制对生成的密钥的访问.
2. 将 Amazon S3 服务器端加密与客户管理的密钥一起使用,并使用以高可用性模式配置的两个 AWS CloudHSM 实例来管理密钥.使用 IAM 来控制对 CloudHSM 中生成的密钥的访问.

答案: BD

解释:

A.S3 生成的密钥无法管理 C.一个 HSM 不是 HA E.CloudHSM 无法与任何 AWS 服务通信

Question 68 **12/12考试原题**

公司运行面向公众的应用程序,该应用程序通过 RESTful 使用基于 Java 的 Web 服务

API.它托管在数据中心中一台服务器上的 Apache Tomcat 上,该服务器始终以 30%的 CPU 使用率运行. 随着新产品的发布,API 的使用有望增加 10 倍.企业希望在不中断的情况下将应用程序迁移到 AWS,并需要对其进行扩展以满足需求.

该公司已经决定使用 Amazon Route 53 和 CNAME 记录来重定向流量.用最少的努力如何满足这些要求?

1. 使用 AWS Elastic Beanstalk 部署 Java Web 服务并启用 Auto Scaling.然后将应用程序切换为使用新的 Web 服务.
2. 使用 AWS SMS 将 Apache 服务器提升并转移到云中.然后,切换应用程序以将 Web 服务流量定向到新实例.
3. 创建一个 Docker 映像并将该映像迁移到 Amazon ECS.然后更改应用程序代码以将 Web 服务查询定向到 ECS 容器.
4. 修改应用程序以通过 Amazon API Gateway 调用 Web 服务.然后创建一个新的 AWS Lambda Java 函数以运行 Java Web 服务代码.测试后,更改 API Gateway 以使用Lambda 函数.

答案: A

解释:

A.这是最好的,因为重新平台有意义.B.重新托管可能不会有太大改善 C.将需要负载平衡器和自动缩放.D.

重新架构需要进行大量工作

Question 69

一家公司正在使用 AWS 进行生产和开发工作负载.每个业务部门都有自己的 AWS 帐户用于生产,还有一个单独的 AWS 帐户用于开发和部署其应用程序.信息安全部门引入了新的安全策略,该策略将访问权限限制为安全团队中一小部分人终止所有帐户中的某些 Amazon EC 实例.

解决方案架构师如何满足这些要求?

1. 创建一个新的 IAM 策略,该策略仅允许安全团队访问那些 EC2 实例.

将此策略应用于 AWS Organizations 主账户.

1. 创建一个新的基于标签的 IAM 策略,该策略仅允许安全团队访问这些 EC2 实例.适当标记实例,然后在每个帐户中应用此策略.
2. 在 AWS Organizations 下创建一个组织单位.将所有帐户移至该组织单位,并使用 SCP 应用白名单策略, 以仅允许安全团队访问这些 EC2 实例.
3. 为 AWS 中的所有账户设置 SAML 联盟.配置 SAML,以便它在验证用户身份之前检查服务 API 调用.如果安全团队以外的任何人访问这些实例,则阻止SAML 对 API 调用进行身份验证.

答案: B

解释:

A.IAM 策略将不会应用于子帐户 C.SCP 不适用于粒度访问控制. SCP 实际上不会同样授予权限https://docs.aws.amazon.com/organizations/latest/userguide/orgs\_manage\_policies\_scp.htmlD.这不会 起作用,因为 SAML 会像令牌基础服务一样工作,并且不依赖 API 调用

Question 70 **12/12考试原题 03/09考试原题 03/23考题**

一家公司正在将关键业务的多层应用程序迁移到 AWS.该体系结构由桌面客户端应用程序和服务器基础结构组成.服务器基础结构位于本地数据中心中,该数据中心经常无法将应用程序正常运行时间 SLA 维持在 99.95%.解决方案架构师必须重新设计应用程序,以确保它可以达到或超过 SLA.

该应用程序包含在单个虚拟机上运行的 PostgreSQL 数据库.业务逻辑和表示层在多个虚拟机之间实现负载平衡.远程用户抱怨使用此延迟敏感型应用程序时加载时间慢.

在改善用户体验和最小化成本的同时,以下哪一项将满足可用性要求,而对应用程序所做的更改很少?

1. 将数据库迁移到 Amazon EC2 中的 PostgreSQL 数据库.将应用程序和表示层托管在 Application Load Balancer 之后的自动缩放的 Amazon ECS 容器中.为每个最终用户分配一个 Amazon WorkSpaces WorkSpace,以提高体验.
2. 将数据库迁移到 Amazon RDS Aurora PostgreSQL 配置.在应用程序负载平衡器后面的 Amazon EC2 实例上,将应用程序和表示层托管在 Auto Scaling 配置中.使用 Amazon AppStream 2.0 改善用户体验.

C.将数据库迁移到 Amazon RDS PostgreSQL 多可用区配置.将应用程序和表示层托管在网络负载平衡器后面的自动缩放的 AWS Fargate 容器中.

使用 Amazon ElastiCache 改善用户体验.

D.将数据库迁移到具有至少两个节点的 Amazon Redshift 集群.在应用程序负载平衡器后面的自动缩放的 Amazon ECS 容器中组合和托管应用程序和表示层.使用 Amazon CloudFront 改善用户体验.

答案: B

解释:

A.EC2 中的数据库可能不是最佳选择 C.使用 ElastiCache 将需要对应用程序进行一些更改 D.Redshift 并非为此设计.即使可行,价格也很高.

Question 71

一家咨询公司正在为其受监管的金融服务用户创建安全的数据分析解决方案.用户将其原始数据上传到仅具有 PutObject 权限的Amazon S3 存储桶.数据将由在 VPC 中启动的 Amazon EMR 集群上运行的应用程序进行分析.公司要求环境与 Internet 隔离.必须使用公司控制的密钥对所有静态数据进行加密.

解决方案架构师应采取哪种行动组合来满足用户的安全要求? (选择两个.)

1. 在配置为使用 AWS KMS CMK 进行 Atrest 加密的专用子网中启动 Amazon EMR 集群. 为 Amazon S3 配置网关 VPC 终端节点,为 AWS KMS 配置接口 VPC 终端节点.
2. 在配置为使用 AWS KMS CMK 进行 Atrest 加密的专用子网中启动 Amazon EMR 集群. 为 Amazon S3 和 NAT 网关配置网关 VPC 终端节点以访问 AWS KMS.
3. 在配置为使用 AWS CloudHSM 设备进行静态加密的专用子网中启动 Amazon EMR 集群. 为 Amazon S3 配置网关 VPC 终端节点,为 CloudHSM 配置接口 VPC 终端节点.
4. 配置 S3 端点策略以仅允许访问必要的数据桶.
5. 配置 S3 存储桶策略以允许使用 aws:sourceVpce 条件进行访问以匹配 S3 端点 ID.

答案: BD → **变更AE**

Question 72 **12/12考试原题** **11/19考试原题 03/09考试原题**

一家公司正在 AWS 上设计一个新的高度可用的 Web 应用程序.该应用程序需要从 AWS 中的应用程序服务器到公司的本地环境中托管的后端 REST API 的一致且可靠的连接. AWS 和本地之间的后端连接将通过私有虚拟接口通过 AWS Direct Connect 连接进行路由. Amazon Route 53 将用于管理应用程序的私有 DNS 记录,以解析后端 REST API 上的 IP 地址.

哪种设计可以提供与后端 API 的可靠连接?

1. 为后端 REST API 至少实现两个后端端点,并使用 Route 53 运行状况检查来监视每个后端端点的可用性并执行 DNS 级别的故障转移.
2. 从另一个网络运营商安装第二个 Direct Connect 连接,并将其连接到与第一个 Direct Connect 连接相同的虚拟专用网关.
3. 为来自同一网络运营商的同一直接连接连接安装第二个交叉连接,并将两个连接都连接到同一私有虚拟 接口上的同一链路聚合组(LAG).
4. 创建从本地数据中心到 AWS 的通过公共 Internet 路由的 IPSec VPN 连接,并将其连接到与 Direct Connect 连接相同的虚拟专用网关.

答 案 : B

Question 73  **03/09考试原题**

公司拥有一个数据中心,必须尽快将其迁移到 AWS.数据中心具有 500 Mbps 的 AWS Direct Connect 链接和单独的,完全可用的 1 Gbps ISP 连接.解决方案架构师必须将 20 TB 的数据从数据中心传输到Amazon S3 存储桶.

什么是最快的数据传输方式?

1. 使用现有的 DX 链接将数据上传到 S3 存储桶.
2. 使用 AWS Import / Export 服务将数据发送到 AWS.
3. 使用 80 TB AWS Snowball 设备上传数据.
4. 使用 S3 传输加速将数据上传到 S3 存储桶. 答案: D

Question 74 **12/12考试原题** **11/19考试原题**  **03/09考试原题**

一家银行正在设计一个在线客户服务门户,客户可以在其中与客户服务代理聊天.如果发生区域性灾难,门户网站必须维持 15 分钟的 RPO 或 RTO.银行法规要求,所有客户服务聊天记录必须在持久性存储中保存至少 7 年,聊天对话必须在飞行中进行加密,而谈话记录必须在静止时进行加密.数据丢失防护小组要求静止数据必须使用该小组控制,旋转和吊销的密钥进行加密.

哪种设计满足这些要求?

1. 聊天应用程序会将每个聊天消息记录到 Amazon CloudWatch Logs 中.预定的 AWS

Lambda 函数调用 CloudWatch Logs.每 5 分钟创建一次 CreateExportTask,以将聊天记录导出到Amazon S3. S3 存储桶已配置为跨区域复制到备份区域.为 CloudWatch Logs 组和 S3 存储桶指定了单独的 AWS KMS 密钥.

1. 聊天应用程序将每个聊天消息记录到两个不同的 Amazon CloudWatch Logs 组中

在两个不同的区域中,应用了相同的 AWS KMS 密钥.两个 CloudWatch Logs 组均配置为将日志导出到具有 7 年保管库锁定策略且指定了 KMS 密钥的 Amazon Glacier 保管库.

1. 聊天应用程序将每个聊天消息记录到 Amazon CloudWatch Logs 中. CloudWatch Logs 组上的订阅过滤器将输入到 Amazon Kinesis Data Firehose,后者会将聊天消息流式传输到备份区域中的 Amazon S3 存储桶.为 CloudWatch Logs 组和 Kinesis Data Firehose 指定了单独的 AWS KMS 密钥.
2. 聊天应用程序将每个聊天消息记录到 Amazon CloudWatch Logs 中. CloudWatch Logs 组配置为使用7 年保管库锁定策略将日志导出到 Amazon Glacier 保管库. Glacier 跨区域复制将聊天档案镜像到备份区域.为 CloudWatch Logs 组和 Amazon Glacier 保管库指定了单独的 AWS KMS 密钥.

答案: C

解释:

A.默认情况下,跨区域复制不会复制 SSE-KMS 对象,这需要通过相关信息(KMS 密钥访问)显式启用.此外, 不支持将 Cloudwatch 导出到 SSE-KMS 加密的 S3 https://docs. B.在 S3 Glacier 之前,您无法直接从cloudwatch 导出到冰川,而且,不支持将 cloudwatch 导出到 SSE-KMS 加密的 S3,我将使用相同的方法到冰川并且您不能在整个区域 https://forums.aws.amazon.com/thread.jspa?threadID=287340 C 使用KMSCMK.KinesisFirehose 可以在静止状态下对 S3 进行加密 https://docs.aws.amazon.com / firehose / latest / dev / create- configure.html D.在 S3 Glacier 之前,您无法直接从 cloudwatch 导出到冰川.此外,如果我们谈论的是 S3 冰川,则不支持将 cloudwatch 导出到 SSE-KMS 加密的 S3. cloudwatch 仅在一个区域可用,冰川可能需要数小时才能检索数据,RTO 不能完成 15 分钟

Question 75 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

一家公司当前在 Amazon EC2 上运行一个安全应用程序,该应用程序通过 AWS Direct Connect 从本地位置获取文件,进行处理,然后将其上传到单个 Amazon S3 存储桶.该应用程序使用 HTTPS 进行到 Amazon S3 传输的加密,并使用 S3 服务器端加密进行静态加密.

解决方案架构师应该建议进行以下哪些更改,以使该解决方案更安全而不影响应用程序的性能?

1. 添加一个 NAT 网关.更新 EC2 实例上的安全组,以仅允许访问和访问 S3 IP 范围.配置一个 S3 存储桶策略,该策略仅允许通过 NAT 网关的弹性 IP 地址进行通信.
2. 添加一个 VPC 端点.在 VPC 终端节点上配置终端节点策略,以仅允许访问所需的 Amazon S3 存储桶. 实施 S3 存储桶策略,该策略仅允许从 VPC 的源 IP 范围进行通信.
3. 添加一个 NAT 网关.更新 EC2 实例上的安全组,以仅允许访问和访问S3 IP 范围.配置一个 S3 存储桶策略,该策略仅允许通过本地网络的源公共 IP 地址进行通信.
4. 添加一个 VPC 端点.在 VPC 端点上配置端点策略,以仅允许访问所需的 S3 存储桶.实施 S3 存储桶策略, 该策略仅允许来自 VPC 端点的通信.

答案: D

解释:

A.通过 Internet 进行请求的安全性会更低 B.您不能在 s3 存储桶策略中为 VPC 端点https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html 使用 sourceIp C.与A.aws:sourceVpce 相同

Question 76

作为在 AWS Cloud 中构建大型应用程序的一部分,要求 Solutions Architect 实施外围安全保护.在 AWS

上运行的应用程序具有以下终端节点:

应用程序负载均衡器

Amazon API Gateway 区域终端节点基于弹性 IP 地址的 EC2 实例. Amazon S3 托管的网站.

经典负载均衡器

解决方案架构师必须设计一种解决方案来保护所有列出的 Web 前端,并提供以下安全功能: DDoS 保护

SQL 注入保护

IP 地址白名单/黑名单 HTTP 泛洪保护无效的机器人抓取工具防护

解决方案架构师应如何设计解决方案?

1. 在所有 Web 终端节点上部署 AWS WAF 和 AWS Shield Advanced.添加 AWS WAF 规则以强制执行公司的要求.
2. 在所有终端节点之前部署 Amazon CloudFront. CloudFront 发行版提供外围保护.添加基于 AWS Lambda 的自动化以提供额外的安全性.
3. 在所有终端节点之前部署 Amazon CloudFront.部署 AWS WAF 和 AWS Shield Advanced.

添加 AWS WAF 规则以强制执行公司的要求.使用 AWS Lambda 自动化并增强安全状况.

1. 通过使用网络 ACL 和安全组并添加规则以强制执行公司的要求来保护端点.使用 AWS Lambda 自动更新规则.

答案: C

解释:

CloudFront 和 AWS Shield Advanced 具有 DDoS 的优势,而 WAF 将支持阻止 IP,SQL 注入攻击和错误的 Bot.

Question 77 **12/12考试原题**

一家公司拥有 100 多个 AWS 账户,每个账户一个 VPC,需要出站

互联网的 HTTPS 连接.当前设计在每个 VPC 中的每个可用区(AZ)包含一个 NAT 网关.为了降低成本并获取有关出站流量的信息,管理层要求提供一种新的 Internet 访问体系结构.

哪种解决方案可以满足当前需求,并随着新帐户的发展而不断发展 供应,同时降低成本?

1. 使用第三方路由设备跨两个可用区创建传输 VPC.创建到每个 VPC 的 VPN 连接.默认将 Internet 流量路由到中转 VPC.
2. 创建多个托管-专用 AWS Direct Connect VIF,每个帐户一个,每个都有一个 Direct Connect 网关.默认将 Internet 流量路由回本地路由器以路由到 Internet.
3. 为出站互联网流量创建一个中央 VPC.使用 VPC 对等可默认路由到中央 VPC 中的一组冗余 NAT 网关.
4. 在中央 VPC 帐户中创建代理机群.在中央VPC 中创建一个 AWS PrivateLink 终端服务.使用

PrivateLink 界面通过代理机群进行 Internet 连接.

答案: A

解释:

A.https://aws.amazon.com/answers/networking/aws-single-region-multi-vpc-connectivity/ B.将流量路由回本地以进行 Internet 访问是一种不良习惯 C.您无法路由流量通过 VPC 对等连接到 NAT 网关https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html D.PrivateLink 无法用于路由互联网流量 https://docs.aws. amazon.com/vpc/latest/userguide/vpce-interface.html

Question 78

一家公司运行带有前端和电子商务层的电子商务平台.这两层都在 LAMP 堆栈上运行,前端实例在负载平衡设备后面运行,该负载平衡设备在 AWS 上具有虚拟产品.当前,运营团队使用 SSH 登录实例以维护补丁并解决其他问题.该平台最近成为多种攻击的目标,包括

DDoS 攻击.

SQL 注入攻击. Web 服务器上的 SSH 帐户多次成功的字典攻击.

该公司希望通过迁移到 AWS 来提高电子商务平台的安全性.该公司的解决方案架构师已决定使用以下方法:

代码检查现有应用程序并解决任何 SQL 注入问题.

将 Web 应用程序迁移到 AWS 并利用最新的 AWS Linux AMI 解决初始安全修补程序.

安装 AWS Systems Manager 来管理修补程序,并允许系统管理员根据需要在所有实例上运行命令. 在提供高可用性并最大程度降低风险的同时,还有哪些其他步骤可以解决所有其他相同的攻击类型呢?

1. 使用限制访问特定 IP 的安全组启用对 Amazon EC2 实例的SSH 访问.将本地 MySQL 迁移到 Amazon RDS Multi-AZ.从 AWS Marketplace 安装第三方负载均衡器,然后将现有规则迁移到负载均衡器的 AWS 实例.启用 AWS Shield Standard 进行 DDoS 保护.
2. 禁用对 Amazon EC2 实例的 SSH 访问.将本地 MySQL 迁移到 Amazon RDS Multi-AZ.利用 Elastic Load Balancer 分散负载并启用 AWS Shield Advanced 进行保护.在网站前面添加 Amazon CloudFront 发行版.在分发上启用 AWS WAF 来管理规则.
3. 通过通过限制对特定 IP 地址的访问来保护的堡垒主机,启用对 Amazon EC2 实例的 SSH 访问.将本地MySQL 迁移到自我管理的 EC2 实例.利用 AWS Elastic Load Balancer 分散负载并启用 AWS Shield Standard 进行 DDoS 保护.

在网站前面添加 Amazon CloudFront 发行版.

1. 禁用对 EC2 实例的SSH 访问.将本地 MySQL 迁移到 Amazon RDS SingleAZ.利用 AWS Elastic Load Balancer 分散负载.在网站前面添加 Amazon CloudFront 发行版.在分发上启用 AWS WAF 来管理规则.

答案: B

解释:

A.我们不再需要 SSH,因为系统管理员可以运行命令并进行补丁. C.我们不再需要 SSH,因为系统管理员可以运行命令并进行补丁.另外带有 ec2 的 mysql 并不是很好的D.RDS Single-AZ 不是 HA

Question 79  **03/09考试原题**

一家公司在其本地数据中心中拥有一个高性能计算(HPC)集群,该集群每月每个星期并行运行数千个作业, 处理 PB 级的图像.映像存储在网络文件服务器上,该服务器被复制到灾难恢复站点.本地数据中心已达到容量,并已开始在一个月的时间内分散作业,以便更好地利用群集,从而导致作业完成延迟.

该公司已要求其解决方案架构师在 AWS 上设计一种经济高效的解决方案,以扩展到目前的 5,000 核和

10 PB 数据容量之外.该解决方案必须需要最少的管理开销,并保持当前的耐用性水平. 哪种解决方案可以满足公司的要求?

1. 在 Amazon Elastic Container Registry 中使用该作业的可执行文件创建一个容器.在 Auto Scaling 组中将 Amazon ECS 与 Spot Fleet 结合使用.将原始数据存储在 Amazon EBS SC1 卷中,并将输出写入Amazon S3.
2. 创建一个结合了按需和预留实例任务节点的 Amazon EMR 集群,这些集群将使用 Spark 从 Amazon S3 中提取数据.使用 Amazon DynamoDB 维护需要由 Amazon EMR 集群处理的作业列表.
3. 将原始数据存储在 Amazon S3 中,并在托管计算环境中使用 AWS Batch 创建 Spot Fleets.将作业提交到 AWS Batch Job Queues,以将对象从 Amazon S3 下拉到 Amazon EBS 卷上以进行临时存储,然后将结果写回到 Amazon S3.
4. 将要处理的作业列表提交给 Amazon SQS,以将需要处理的作业排队.使用 Spot Fleet 创建一个多样化的 Amazon EC2 worker 实例集群,该集群将根据队列深度自动扩展.使用 Amazon EFS 存储在集群中所有实例之间共享的所有数据.

答案: C

解释:

A.这很难执行和维护,因为 EBS 的最大大小限制为 16TB,并且无法安装到多个实例 B.DynamoDb 并不是最终存储作业项目的最佳场所,因为它具有最终一致性的性质 D.S3 可能更好这里的存储选项

Question 80

一家大公司有许多业务部门.每个业务部门都有多个用于不同目的的 AWS 账户.该公司的 CIO 认为,每个业务部门都有可用于与该公司其他部门共享的数据,在 1000 个 AWS 账户中,大约有 10 PB 的数据需要与用户共享.数据是专有的,因此其中的某些数据仅应提供给具有特定工作类型的用户.一些数据用于密集工作量的吞吐量,例如模拟.由于新的计划,收购和资产剥离,帐户数量经常变化.

已要求解决方案架构师设计一个系统,该系统允许与公司中的所有员工共享在 AWS 中使用的数据. 哪种方法将允许以可扩展方式共享安全数据?

A.将数据存储在单个 Amazon S3 存储桶中.为作业类型和业务单位的每种组合创建一个 IAM 角色,该角色允许根据 S3 存储桶中的对象前缀进行适当的读/写访问.

角色应具有允许业务部门的 AWS 账户承担其职责的信任策略角色.

在每个业务部门的 AWS 账户中使用 IAM,以防止他们担任其他工作类型的角色.用户可以通过其业务部门的 AWS 账户使用 AssumeRole 获得凭据来访问数据.然后,用户可以将这些凭据与 S3 客户端一起使用. B.将数据存储在单个 Amazon S3 存储桶中.编写一个存储桶策略,该策略使用条件根据每个用户的业务部门和作业类型在适当的情况下授予读写访问权限.确定具有访问存储段的 AWS 账户和 IAM 用户名中带有

前缀的作业类型的业务单位.用户可以通过 S3 客户端使用其业务部门的 AWS 账户中的 IAM 凭据来访问数据.

1. 将数据存储在一系列 Amazon S3 存储桶中.创建在Amazon EC2 中运行的应用程序,该应用程序与公司的身份提供程序(IdP)集成在一起,该应用程序对用户进行身份验证,并允许他们通过该应用程序下载或上传数据.该应用程序使用 IdP 中的业务部门和职位类型信息来控制用户可以通过该应用程序上传和下载的内容.用户可以通过应用程序的 API 访问数据.
2. 将数据存储在一系列 Amazon S3 存储桶中.创建与公司的身份提供商(IdP)集成的*AWS STS 令牌自动售货机.*当用户登录时,让令牌自动售货机附加一个 IAM 策略,该策略承担限制用户访问和/或仅上传用户有权访问的数据的角色.用户可以通过对令牌自动售货机的网站或 API 进行身份验证来获取凭据,然后将这些凭据用于 S3 客户端.

答案: D

解释:

A.为了获得最佳实践,我们应该使用 IAM 角色.但是,此解决方案意味着每次添加一个帐户时,我们都需要为该帐户中的所有作业类型创建角色,并且在该帐户中,我们需要附加IAM 策略,以防止它们承担其他作业类型角色.这可能是很多工作. B.his 不是理想的解决方案,但是当我们添加或删除帐户时,它只需很少的精力. 我们可以使用拒绝规则来通过拒绝不在列表中的帐户或职位类型来实现此目的.一个存储桶中的 10PB 似乎太多了,每次新公司加入时,我们都需要更新政策. C.过多的开销. D.token 自动售货机主要用于移动应用程序,我认为这不是一个很好的解决方案.但是,在管理方面,我认为这是最好的解决方案

Question 81 **11/19考试原题 03/23考题**

一家公司希望将其网站从本地数据中心迁移到 AWS.同时,它希望将网站迁移到基于容器的基于微服务的架构,以提高可用性和成本效率.该公司的安全策略规定,必须根据最佳实践使用最少的特权来配置特权和网络许可.

解决方案架构师必须创建一个满足安全要求的容器化架构,并将该应用程序部署到 Amazon ECS 集群. 部署后需要执行哪些步骤才能满足要求? (选择两个.)

1. 使用网桥网络模式创建任务.
2. 使用 awsvpc 网络模式创建任务.
3. 将安全组应用于 Amazon EC2 实例,并对 EC2 实例使用 IAM 角色来访问其他资源. D.将安全组应用于任务,并在启动时将 IAM 凭据传递到容器中以访问其他资源.

E.将安全组应用于任务,并将 IAM 角色用于任务以访问其他资源.

答案: BE

解释:

A.由于在桥接模式下,同一实例中的所有容器都共享该实例的同一安全组,因此我们可以打开不必要的端 口.对于最低特权来说,这是不好的. B.由于每个任务都有自己的 ENI 和安全组,因此我们可以在这里进行细粒度的许可 C.如果不选择 A,则没有必要.D.传递 IAM 凭据是不道德的行为 E.https://docs. aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html

Question 82 **12/12考试原题**

一家公司正在将其营销网站和内容管理系统从本地数据中心迁移到 AWS.该公司希望使用带有 Web 服务器的 Amazon EC2 实例和用于数据库的Amazon RDS 实例在 VPC 中开发 AWS 应用程序.

该公司有一个运行手册文档,描述了本地系统的安装过程.该公司希望将 AWS 系统基于 Runbook 文档中引用的流程.该运行手册文档描述了服务器上操作系统的安装和配置,网络设置,网站以及内容管理系统软 件.迁移完成后,该公司希望能够快速进行更改以利用其他 AWS 功能.

如何在 AWS 中部署和自动化应用程序和环境,同时允许将来进行更改?

1. 更新运行手册,以描述如何使用 AWS 控制台为应用程序创建 VPC,EC2 实例和 RDS 实例.确保更新了运行手册中的其余步骤,以反映可能来自 AWS 迁移的任何更改.
2. 编写一个 Python 脚本,该脚本使用 AWS API 为应用程序创建 VPC,EC2 实例和 RDS 实例.编写用于实现 Runbook 中其余步骤的 Shell 脚本.让 Python 脚本复制并在新创建的实例上运行 Shell 脚本以完成安装.
3. 编写一个 AWS CloudFormation 模板,该模板为应用程序创建 VPC,EC2 实例和 RDS 实例.确保更新了运行手册中的其余步骤,以反映可能来自 AWS 迁移的任何更改.
4. 编写一个 AWS CloudFormation 模板,该模板为应用程序创建 VPC,EC2 实例和 RDS 实例.在 AWS CloudFormation 模板中包括 EC2 用户数据以安装和配置软件.

答案: D

解释:

A.不是最佳解决方案 B.Cloudformation 是更好的选择 C.我们可以使其余步骤自动化D.https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html

Question 83 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

一家公司正在添加新的批准的仅支持 IPv6 连接的外部供应商.该公司的后端系统位于 Amazon VPC 的专用子网中.该公司使用 NAT 网关来允许这些系统通过 IPv4 与外部供应商进行通信.公司政策要求与外部供应商进行通信的系统使用安全组,该安全组将访问权限限制为仅允许批准的外部供应商.虚拟私有云(VPC)使用默认的网络 ACL.

系统操作员已成功将 IPv6 地址分配给每个后端系统.系统操作员还更新出站安全组,以包括外部供应商

(目的地)的 IPv6 CIDR. VPC 中的系统能够通过 IPv6 成功 ping 通彼此.但是,这些系统无法与外部供应商进行通信.

要与外部供应商进行通信,需要进行哪些更改?

1. 创建一个 IPv6 NAT 实例.为目标 0.0.0.0/0 添加指向 NAT 实例的路由.
2. 在 NAT 网关上启用 IPv6.为目标:: / 0 指向 NAT 网关添加路由.
3. 在互联网网关上启用 IPv6.添加指向目标 IGW 的目的地 0.0.0.0/0 的路由. D.创建一个仅出口的互联网网关.为指向网关的目标:: / 0 添加路由.

答案: D

解释:

Nat 网 关 或 Nat 实 例 不 支 持 IPv6 https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_NAT\_Instance.html https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

Question 84 **11/19考试原题 03/23考题**

一家金融公司正在当前的 Linux EC2 实例上运行其业务关键型应用程序.该应用程序包括一个自我管理的 MySQL 数据库,该数据库执行繁重的 I / O 操作.该应用程序可以正常工作,以在一个月内处理少量流量.

但是,由于月末报告,它在每月的最后三天内变慢,即使该公司在其基础架构中使用弹性负载平衡器和 Auto Scaling 来满足不断增长的需求.

以下哪个操作将允许数据库处理对性能有最小影响的月末负载?

1. 使用更大的实例类型预热 Elastic Load Balancer,将所有 Amazon EBS 卷更改为 GP2 卷.
2. 执行一次数据库集群到 Amazon RDS 的迁移,并创建多个其他只读副本来处理月底期间的负载. C.将 Amazon CloudWatch 与 AWS Lambda 结合使用,以基于特定 CloudWatch 指标更改集群中Amazon EBS 卷的类型,大小或 IOPS.

D.通过在月底之前拍摄快照,然后在之后还原,将所有现有的Amazon EBS 卷替换为具有最大可用存储大小和每秒 I / O 的新 PIOPS 卷.

答案: B

Question 85 **12/12考试原题**  **03/09考试原题**

解决方案架构师正在设计用于数据仓库应用程序的存储层.数据文件很大,但是它们在每个文件的开头都有静态放置的元数据,用于描述文件索引的大小和位置.一系列 Amazon EC2 实例读取数据文件,这些实例将索引大小,索引位置以及有关数据文件的其他类别信息存储在数据库中. Amazon EMR 使用该数据库将文件分组在一起,以进行更深入的分析.

对于此工作流程,最有成本效益的高可用性存储解决方案是什么?

A.将数据文件存储在 Amazon S3 中,并对每个文件的元数据使用Range GET,然后为相关数据建立索引. B.将数据文件存储在由 EC2 舰队和 EMR 节点安装的 Amazon EFS 中.

C.将数据文件存储在 Amazon EBS 卷上,并允许EC2 舰队和 EMR 在需要它们的卷上进行装载和卸载. D.将数据文件的内容存储在 Amazon DynamoDB 表中,并将元数据,索引和数据作为其自己的键.

答案: A

解释:

S3 对象数据将非常适合此处,因为我们可以进行范围获取,因此不需要加载元数据信息文件. https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectGET.html

Question 86 **11/19考试原题**

一家公司每天使用 Amazon EMR 集群处理数据.原始数据来自 Amazon S3,生成的处理后数据也存储在Amazon S3 中.处理必须在 4 小时内完成；目前只需要 3 个小时.但是,处理时间需要 5 到 10 分钟.由于原始数据量的增加,每周需要更长的时间.

该团队还担心随着计算能力的增加而成本上升. EMR 群集当前在三个 m3 xlarge 实例(一个主节点和两个核心节点)上运行.

以下哪种解决方案将减少与不断增长的计算需求相关的成本?

1. 添加其他任务节点,但让团队为每个其他节点购买一个可预先转换的全保留实例,以抵消成本.
2. 添加其他任务节点,但将实例队列与主节点按需模式一起使用,并将核心节点和任务节点的按需实例和 竞价型实例混合使用.为主节点购买计划的预留实例.
3. 添加其他任务节点,但在主节点处于竞价模式下并结合按需实例和竞价型实例用于核心节点和任务节点 的情况下,使用实例队列.购买足够的预定预留实例,以抵消运行任何按需实例的成本.
4. 添加其他任务节点,但在主节点处于按需模式下将实例队列与主节点一起使用,并且将核心节点和任务 节点的按需实例和竞价型实例混合使用.为主节点购买标准的allupfront 预留实例.

答案: B

解释:

A.Spot 实例会更便宜 C.Master 节点不应该是 Spot 实例 D.所有预付款都应该比预定的预留设备贵

Question 87 **11/19考试原题 03/23考题**

一家公司正在构建一个 AWS 登陆区域,并已要求解决方案架构师设计一种多账户访问策略,该策略将允许数百名用户使用公司凭证来访问 AWS 控制台.该公司正在运行 Microsoft Active Directory,用户将使用AWS Direct Connect 连接来连接到 AWS.该公司还希望能够与第三方服务和提供商(包括自定义应用程序)建立联盟.

哪种解决方案使用最少的管理开销就能满足要求?

1. 通过使用单一登录和带有 SAML 2.0 的 Active Directory 联合身份验证服务(AD FS),将 Active Directory 连接到AWS,然后将身份提供程序(IdP)系统配置为使用基于表单的身份验证.使用公司品牌构建 AD FS 门户页面,并根据需要集成支持 SAML 2.0 的第三方应用程序.
2. 在本地 Active Directory 和 AWS Directory Service 之间创建双向森林信任关系.使用 AWS Organizations 设置 AWS Single Sign-On.将单点登录集成用于与第三方应用程序的连接.
3. 通过使用 AWS Directory Service AD 连接器连接本地 Active Directory 来配置单一登录.通过使用 IAM

应用程序和服务链接功能,启用与AWS 服务和账户的联合.根据需要利用第三方单点登录.

1. 通过使用 AD FS 和 SAML 2.0 将公司的 Active Directory 连接到 AWS.配置 AD FS 声明规则以根据需要利用 Regex 第三方单点登录,并将其添加到 AD FS 服务器.

答案: B

解释:

A.这将起作用,但是您需要在本地环境中构建登录页面,并在 AD FS 门户页面和 AD FS 服务器中构建 C. 我不认为这种方式使用了服务链接功能.我们应该将 AWS SSO 用于联盟,以便我们可以利用第三方 SSO. https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html https://aws.amazon.com/blogs/security/how-to-create-and-manage -users-within-aws-sso /D.将需要维护 AD FS 服务器

Question 88 **11/19考试原题**

解决方案架构师正在为一家公司提供网络解决方案,该公司的应用程序正在北弗吉尼亚州的数据中心中运 行.该公司数据中心中的应用程序要求对在 useast-1 中的虚拟私有云(VPC)和在同一帐户中的 uswest-2 中的辅助 VPC 中运行的应用程序具有可预测的性能.公司数据中心位于服务于 us-est-1 区域的 AWS Direct Connect 设施中.该公司已经订购了 AWS Direct Connect 连接,并且已经建立了交叉连接.

哪种解决方案将以最低的成本满足要求?

1. 提供一个 Direct Connect 网关,并在 us-east-1 中为 VPC 附加虚拟专用(VGW),在 us-west-2 中为 VPC

附加 VGW.在 Direct Connect 连接上创建专用 VIF,并将其关联到 Direct Connect 网关.

1. 在 usest-1 和 us-west-2 区域的公司的每个 VPC 的直接连接连接上创建专用 VIF.将公司的数据中心路由器配置为通过专用 VIF 直接与这些区域中的 VPC 连接.
2. 在 us-east-1 区域中使用基于 Amazon EC2 的路由器实例部署中转 VPC 解决方案. 在转接路由器和虚拟专用网关(VGW)之间建立 IPsec VPN 隧道

位于 us-east-1 和 us-west-2 地区,这些地区与公司在这些地区的 VPC 相连.

在 Direct Connect 连接上创建公用 VIF,并在转接路由器和公司数据中心路由器之间的公用 VIF 上建立

IPsec VPN 隧道.

1. 订购第二条 Direct Connect 连接到 Direct Connect 设施,并连接到 uswest-2 区域.与合作伙伴一起建立从 Direct Connect 设施到公司数据中心的暗光纤网络扩展链接.在直连连接上为各个地区的每个公司VPC 建立专用 VIF.将公司的数据中心路由器配置为通过专用VIF 直接与这些区域中的 VPC 连接.

答案: A

解释:

* 1. irect Connect 网关是全局资源,这使得与其他区域的连接也很

快 .https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html BA 越少越好延迟 https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface- dx/ CI 我们认为这里不需要公共 VIF.同样,维护 EC2 服务器也是开销. D.这可以用,但是 A 便宜很多

Question 89

公司在以下两个 AWS 区域中部署了 Web 服务:us-west-2 和 us-est1.每个 AWS 区域都运行相同版本的

Web 服务. Amazon Route 53 用于将客户路由到延迟最短的 AWS 区域. 该公司希望提高 Web 服务的可用性,以防两个 AWS 区域之一发生中断.

解决方案架构师建议执行 Route 53 健康检查.健康检查必须在端点上检测到特定文本. 端点应满足什么条件组合才能通过 Route 53 健康检查? (选择两个.)

1. 端点必须在 10 秒内建立 TCP 连接.
2. 端点必须返回 HTTP 200 状态代码.
3. 端点必须返回 HTTP 2xx 或 3xx 状态代码.
4. 特定的文本字符串必须出现在响应的前 5120 个字节内. E.端点必须在创建健康检查时指定的秒数内响应请求.

答案: CD

解释:

A.限制为 4 秒 B.2xx 或 3xx 是好的. E.必须在 2 秒内回复https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of- endpoints.html#dns-failover-determining-health-of-endpoints-monitor-endpoint

Question 90

在 AWS 上运营网站的公司需要高度的可扩展性,可用性和性能.该公司正在 Amazon EC2 上运行 Ruby on Rails 应用程序.它在 Amazon EC2 上的 MySQL 5.6 上具有数据层,使用 16 TB Amazon EBS 存

储.Amazon CloudFront 用于缓存应用程序内容.运营团队报告了分配给 MySQL 数据库的 EBS 卷的持续和意外增长.解决方案架构师已被要求设计一个高度可扩展,高度可用和高性能的解决方案.

哪种解决方案在规模上最具成本效益?

1. 对当前配置中的所有 EC2 实例实施多可用区和自动缩放.确保所有 EC2 实例均作为保留实例购买.为数据层实施新的弹性 Amazon EBS 卷.
2. 使用 Amazon ECS 为应用程序设计和实施基于Docker 的容器化解决方案.

迁移到 Amazon Aurora MySQL Multi-AZ 集群.根据需要实施针对 Aurora MySQL 存储使用情况的存储检查以及 AWS Lambda 函数以扩展 Aurora MySQL 存储.

确保实现了多可用区架构.

1. 确保 EC2 实例的大小合适,并且在 Elastic Load Balancing 负载均衡器的后面.使用 EC2 实例实施 Auto Scaling.确保购买的预留实例具有固定容量,并且 Auto Scaling 实例按需运行.迁移到 Amazon Aurora MySQL Multi-AZ 集群.确保实现了多可用区架构.
2. 确保 EC2 实例大小合适并且在 Elastic Load Balancer 后面.使用 EC2 实例实施 Auto Scaling.确保购买的预留实例具有固定容量,并且 Auto Scaling 实例按需运行.迁移到 Amazon Aurora MySQL Multi-AZ 集群.

根据需要实施针对 Aurora MySQL 存储利用率的存储检查以及AWS Lambda 函数以扩展 Aurora MySQL 存储.确保实现了多可用区架构.

答案: C

解释:

A.带有 EC2 的数据库非常昂贵,EBS 的最大大小为 16TB.B.Aurora 存储可以自动分配https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/ Aurora.Managing.Performance.html＃Aurora. D.Aurora 存储可以自动进行管理,性能,存储扩展

Question 91 **12/12考试原题**  **03/09考试原题**

安全团队需要为实习生团队提供一个 AWS 环境,以便他们可以构建无服务器视频转码应用程序.该项目将使用 Amazon S3,AWS Lambda,Amazon API 网关,Amazon Cognito,Amazon DynamoDB 和 Amazon Elastic Transcoder.

实习生应该能够创建和配置必要的资源,但是他们可能无权创建或修改 AWS IAM 角色.解决方案架构师创建策略并将其附加到实习生小组.

安全团队应如何配置环境以确保实习生自给自足?

A.创建一个仅允许创建与项目相关的资源的策略.创建具有所需服务权限的角色,这些权限可由服务承担. B.创建一个策略,该策略允许创建所有与项目相关的资源,包括仅允许访问指定资源的角色.

1. 创建具有所需服务权限的角色,这些权限可由服务承担.让实习生创建并使用堡垒主机仅在项目子网中 创建项目资源.
2. 创建一个仅允许创建与项目相关的资源的策略.要求实习生提出要与安全团队一起创建角色的请求.实 习生将提供在角色中设置权限的要求.

答案: A

解释:

B.Intern 不应该访问 IAMC.这是行不通的.提到的某些资源是全局资源,它们不属于子网或 VPC,您将需要IAM 来执行此操作,而不仅仅是堡垒服务器. D.筹款要求不足够

Question 92

一家公司正在 Amazon EC2 上运行商业 Apache Hadoop 集群.每天都使用此集群来查询 Amazon S3 上的大文件. Amazon S3 上的数据已经过整理,不需要任何其他转换步骤.该公司正在使用 Amazon EC2 上的商业商务智能(BI)工具来对 Hadoop 集群运行查询并可视化数据.

该公司希望减少或消除与管理 Hadoop 群集和 BI 工具相关的间接费用.该公司希望以最小的努力将其迁移至更具成本效益的解决方案.可视化很简单,只需要执行一些基本的聚合步骤即可.

哪个选项可以满足公司的要求?

1. 每天启动一个临时 Amazon EMR 集群,并开发一个 Apache Hive 脚本来分析 Amazon S3 上的文件.作业完成后,关闭 Amazon EMR 集群.使用 Amazon QuickSight 连接到 Amazon EMR 并执行可视化.
2. 开发一个存储过程,该存储过程从在 Amazon EC2 上运行的 MySQL 数据库调用,以分析 EC2 来分析

Amazon S3 中的文件.然后使用在 Amazon EC2 上运行的快速内存 BL 工具来可视化数据.

1. 开发一个脚本,该脚本使用 Amazon Athena 查询和分析 Amazon S3 上的文件.然后使用 Amazon QuickSight 连接到 Athena 并执行可视化.
2. 使用在 Amazon EC2 上运行的商业提取,转换,加载(ETL)工具准备要处理的数据.然后切换到运行在

Amazon EC2 上的更快,更便宜的 Bl 工具,以可视化来自 Amazon S3 的数据.

答案: C

解释:

A 这可能有效,但每天的 EMR 旋转仍然很昂贵.另外,要将 Quicksight 连接到 EMR,您将需要在集群中预先运行. B.这很糟糕.而且我认为您无法从存储的过程中访问 s3 . D.Bad 练习. ETL 可能需要很长时间.

Question 93 **12/12考试原题**  **03/09考试原题**

一家大型跨国公司在 AWS 上运行时间表应用程序,全世界的员工都在使用该应用程序.该应用程序在弹性负载平衡(ELB)负载均衡器后面的 Auto Scaling 组中的 Amazon EC2 实例上运行,并存储在 Amazon RDS MySQL Multi-AZ 数据库实例中.

如果该应用程序不可用,CFO 会担心对业务的影响.应用程序停机的时间不得超过两个小时,但是解决方案必须尽可能具有成本效益.

解决方案架构师应如何满足 CFO 的要求,同时最大程度地减少数据丢失?

1. 在另一个区域中,配置只读副本并创建基础结构的副本.发生问题时,请升级只读副本并将其配置为Amazon RDS Multi-AZ 数据库实例.更新 DNS 以指向其他区域的 ELB.
2. 为 Amazon RDS Multi-AZ 数据库实例配置 60 分钟快照的 1 天窗口.

创建使用最新快照的应用程序基础架构的 AWS CloudFormation 模板.发生问题时,请使用AWS CloudFormation 模板在另一个区域中创建环境.更新 DNS 记录以指向其他区域的 ELB.

1. 配置复制到另一个区域的 Amazon RDS Multi-AZ 数据库实例的 60 分钟快照的 1 天窗口.创建使用最新复制的快照的应用程序基础架构的 AWS CloudFormation 模板.发生问题时,请使用 AWS CloudFormation 模板在另一个区域中创建环境.更新 DNS 记录以指向其他区域的 ELB.
2. 在另一个区域中配置一个只读副本.创建应用程序基础架构的 AWS CloudFormation 模板.发生问题时, 升级只读副本并将其配置为 Amazon RDS Multi-AZ 数据库实例,并使用 AWS CloudFormation 模板使用升级的 Amazon RDS 实例在另一个区域中创建环境.更新 DNS 记录以指向其他区域的 ELB.

答案: D

解释:

A.多站点很昂贵,我们可能在 2 小时内不需要 RTOB.在后台,快照是区域资源,您需要复制到其他区域才能使用它. C.与 D 相比,可能会丢失 1 小时的数据. D.这是典型的指示灯结构,几乎没有数据丢失

Question 94

一个开发团队创建了一系列 AWS CloudFormation 模板来帮助部署服务.他们为网络/虚拟专用(VPC)堆栈,数据库堆栈,堡垒主机堆栈和特定于 Web 应用程序的堆栈创建了模板.每个服务至少需要部署:

网络/ VPC 堆栈堡垒主机堆栈 Web 应用程序堆栈

每个模板都有多个输入参数,这使得很难从 AWS CloudFormation 控制台单独部署服务.一个堆栈的输入参数通常是其他堆栈的输出.例如,可能需要在应用程序堆栈或数据库堆栈中使用网络堆栈中的 VPC ID, 子网 ID 和安全组.

哪些操作将有助于减轻操作负担并减少传递给服务部署的参数数量? (选择两个.)

1. 为每个服务创建一个新的 AWS CloudFormation 模板.在现有模板之后使用交叉堆栈引用来消除将许多参数传递给每个模板.将应用程序的每个必需堆栈作为新堆栈中的嵌套堆栈进行调用.从 AWS CloudFormation 控制台调用新创建的服务堆栈,以使用先前所需参数的子集部署特定服务.
2. 在 AWS Service Catalog 中为每个服务创建一个新的投资组合.为构建服务所需的每个现有 AWS CloudFormation 模板创建产品.将产品添加到在 AWS Service Catalog 中代表该服务的产品组合中.要部署服务,请选择特定的服务组合,然后使用必要的参数启动组合以部署所有模板.
3. 为每个服务设置一个 AWS CodePipeline 工作流.对于每个现有模板,选择 AWS CloudFormation 作为部署操作.将 AWS CloudFormation 模板添加到部署操作中.确保已处理部署操作,以确保遵守相关性.

使用配置文件和脚本在堆栈之间共享参数.要启动服务,请通过选择服务名称并发布更改来执行特定模板. D.使用 AWS Step Functions 定义新服务.为每个服务创建一个新的 AWS CloudFormation 模板.在现有 模板之后使用交叉堆栈引用来消除将许多参数传递给每个模板.从新服务模板中将应用程序的每个必需堆 栈作为嵌套堆栈进行调用.配置 AWS Step Functions 以直接调用服务模板.在 AWS Step Functions 控制台中,执行步骤.

E.在 AWS Service Catalog 中为服务创建新的投资组合.为每个服务创建一个新的 AWS CloudFormation 模板.在现有模板之后使用交叉堆栈引用来消除将许多参数传递给每个模板.将应用程序的每个必需堆栈作为新堆栈中的嵌套堆栈进行调用.为每个应用程序创建一个产品.将服务模板添加到产品.将每个新产品添加到产品组合中.从产品组合中部署产品以使用必要的参数来部署服务,仅用于开始部署.

答案: CE

解释:

A. Cloudformation 控制台不能很好地处理多种服务 B.服务不应该是产品组合,它更像是一种产品.另外,我认为不可能启动投资组合 C.使用 CodePipeline 很好,但是我不愿意与配置文件和脚本共享参数.我们仍然可以使用跨栈引用,但这是最好的两个 D 之一.您不能直接从 Step Function 部署 cloudformation 模板https://docs.aws.amazon.com/step-functions/latest/dg/concepts-service-integrations.html E.带有交叉堆栈的嵌套堆栈参考示例

https://cloudacademy.com/blog/understanding-nested-cloudformation-stacks/

Question 95 **11/19考试原题**

一家公司在负载均衡器后面有一个应用程序,该应用程序具有足够的 Amazon EC2 实例来满足高峰需求. 当需求增加或实例失败时,将使用脚本和第三方部署解决方案来配置EC2 实例.团队必须定期评估实例类型的利用率,以确保部署了正确的大小.

如何优化此工作负载以满足这些要求?

1. 使用 CloudFormer`从当前资源创建 AWS CloudFormation 堆栈.使用同一区域中的 AWS CloudFormation 部署该堆栈.使用 Amazon CloudWatch 警报发送有关未充分利用资源的通知,以提供节省成本的建议.
2. 创建一个 Auto Scaling 组以扩展实例,并使用 AWS CodeDeploy 执行配置.从负载均衡器更改为应用程序负载均衡器.购买第三方产品,该产品可提供有关节省 AWS 资源成本的建议.
3. 通过使用带有默认选项的 AWS Elastic Beanstalk 部署应用程序.注册 AWS

支持开发人员计划.通过使用 Amazon CloudWatch 查看应用程序的实例使用情况,并确定可以处理负载的较便宜的实例.每月举行一次会议,以审查新实例类型并确定是否应购买预留实例.

1. 使用 Amazon ECS 将应用程序部署为 Docker 映像.设置 Amazon EC2 Auto Scaling 和 Amazon ECS 缩放.注册 AWS Business Supp AWS Business Support 并使用 Trusted Advisor 检查以提供有关节省成本的建议

答案: D

解释:

A.我们在这里不需要 cloudformation B.CodeDeploy 并没有真正用于配置基础结构(配置自动伸缩组)C. 这个答案什么都解决不了...

Question 96 **12/12考试原题**

一家大型的全球金融服务公司拥有多个业务部门.该公司希望允许开发人员尝试新服务,但是对于不同的工作负载有多个合规性要求.安全团队关注本地和 AWS 实施的访问策略.他们想对业务团队用于监管工作负载(包括支付卡行业(PCI)要求)的 AWS 服务实施治理.

哪种解决方案可以解决安全团队的疑虑并允许开发人员尝试新服务?

A.实施强大的身份和访问管理模型,其中包括各种 AWS 账户中的用户,组和角色.确保已启用集中式 AWS CloudTrail 日志记录以检测异常.使用 AWS Lambda 构建自动化以拆除未经批准的 AWS 资源进行治理. B.根据业务部门,环境和特定法规要求建立多帐户策略.使用本地身份存储在所有 AWS 账户中实施基于SAML 的联盟.使用 AWS Organizations 并根据法规和服务监管来构建组织单位(OU)结构.跨 OU 实施服务控制策略.

1. 根据业务部门,环境和特定法规要求实施多帐户策略.确保仅允许 PCI 兼容服务在帐户中使用.建立 IAM

策略,仅允许访问符合 PCI 要求的服务以进行管理.

1. 为公司建立一个 AWS 账户以实现强大的安全控制.确保提高所有服务限制以满足公司的可扩展性要求. 使用本地身份存储实施 SAML 联合,并确保帐户中仅使用批准的服务.

答案: B

解释:

B.是否应该尝试从一开始就停止创建服务 C.SCP 更适合这里? D.不是最佳做法

Question 97 **12/12考试原题** **11/19考试原题 类似？**  **03/09考试原题**

一家公司有一个紧迫的期限将其内部部署环境迁移到 AWS.它使用虚拟机导入/导出服务在 Microsoft SQL Server 和 Microsoft Windows Server 上移动,并重建了云本地的其他应用程序.该团队创建了两个Amazon EC2 数据库并使用了 Amazon RDS.公司中的每个团队都负责迁移其应用程序,并希望提出减少其 AWS 支出的建议.

解决方案架构师应采取哪些步骤来降低成本?

1. 启用 AWS 业务支持并查看 AWS Trusted Advisor 的成本检查.为需求波动的应用程序创建 Amazon EC2 Auto Scaling 组.将 AWS Simple Monthly Calculator 报告保存在 Amazon S3 中以进行趋势分析.在" 组织"下创建一个主帐户,并让团队加入以合并帐单.
2. 启用 Cost Explorer 和 AWS Business Support 储备 Amazon EC2 和 Amazon RDS 数据库实例.使用Amazon CloudWatch 和 AWS Trusted Advisor 进行监视并接收节省成本的建议.在"组织"下创建一个主帐户,并让团队加入进行合并计费.
3. 创建一个 AWS Lambda 函数,该函数根据 Amazon CloudWatch 警报更改实例大小.根据 AWS Simple Monthly Calculator 建议保留实例.进行 AWS 精心设计的框架审查并应用建议.在"组织"下创建一个主帐户,并让团队加入进行合并计费.
4. 创建预算并监视超出预算的成本.为需求波动的应用程序创建 Amazon EC2 Auto Scaling 组.创建一个AWS Lambda 函数,该函数根据 Amazon CloudWatch 警报更改实例大小.让每个团队将其账单上传到Amazon S3 存储桶以分析团队支出.在每晚批处理作业上使用竞价型实例.

答案: B

解释:

A.简单的每月执行者报告实际上并不是分析趋势的报告. C.Resize 实例可能需要先停止实例,这对于生产环境而言并不理想.. D.合并帐单是必须的,这是必须的

Question 98 **11/19考试原题 03/23考题**

一家公司希望将其呼叫系统替换为使用 AWS 托管服务构建的解决方案.公司的呼叫中心希望该解决方案能够接听电话,建立联系流以及扩展规模以应对增长预期.呼叫中心还希望该解决方案使用深度学习功能来识别呼叫者的意图并处理基本任务,从而减少与代理通话的需求.该解决方案还应该能够查询业务应用程序,并根据请求将相关信息返回给呼叫.

解决方案架构师应使用哪些服务来构建此解决方案? (选择三个.)

1. Amazon Rekognition 识别正在呼叫的身份.
2. Amazon Connect 创建一个基于云的联络中心.
3. Amazon Alexa for Business 建立对话界面.
4. 与内部系统集成的 AWS Lambda.
5. Amazon Lex 识别呼叫者的意图.
6. Amazon SQS 将传入呼叫者添加到队列中.

答案: BDE

解释:

A.识别适用于图像和视频 B.Amazon connect 是呼叫中心服务 C.Alexa 适用于设备 E.Lex 用于构建会话界面 F.呼叫者队列也由 Amazon connect 管理,并且 SQS 并非为这个.

Question 99 **11/19考试原题**

一家大型公司正在将其整个 IT 产品组合迁移到 AWS.公司中的每个业务部门都有一个独立的 AWS 账户, 同时支持开发和测试环境.很快将需要新的帐户来支持生产工作负载.

财务部门要求采用集中式付款方式,但必须保持对每个组支出的可见性以分配成本. 安全团队需要一个集中的机制来控制公司所有帐户中 IAM 的使用.

通过以下努力,以下选项的组合可以满足公司的需求? (选择两个.)

1. 使用一组参数化的 AWS CloudFormation 模板,这些模板定义了在每个帐户中启动的通用 IAM 权限.要求所有新帐户和现有帐户启动适当的堆栈,以实施最低特权模型.
2. 使用 AWS Organizations 从选定的付款人帐户创建新组织并定义组织单位层次结构.邀请现有帐户加入组织,并使用组织创建新帐户.
3. 要求每个业务部门使用其自己的 AWS 账户.适当标记每个 AWS 账户,并启用 Cost Explorer 来管理退款.
4. 启用 AWS Organizations 的所有功能并建立适当的服务控制策略,以过滤子账户的 IAM 权限.
5. 将公司的所有 AWS 账户整合到一个 AWS 账户中.将标签用于计费目的和 IAM 的访问建议功能可实施最低特权模型.

答案: BD

解释:

A. 这 可 以 工 作 , 但 是 过 程 会 有 些 麻 烦 . C. 我 们 也 希 望 合 并 帐 单 . D.https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-to-set-permission- guardrails-您的组织机构帐户/ E.单一帐户不是一个好选择

Question 100

一家公司每天从 100,000 个源中收集稳定的 1000 万条数据记录.这些记录将写入 Amazon RDS MySQL 数据库.查询必须产生过去 30 天内数据源的每日平均值.读取次数是写入次数的两倍.对收集到的数据的查询一次针对一个源 ID.

解决方案架构师如何提高此解决方案的可靠性和成本效益?

1. 在多可用区模式下将 Amazon Aurora 与 MySQL 一起使用.使用四个其他只读副本.
2. 使用 Amazon DynamoDB,将源 ID 作为分区键,并将时间戳作为排序键. 30 天后,请使用生存时间(TTL) 删除数据.
3. 将 Amazon DynamoDB 与源 ID 用作分区键.每天使用不同的表格.
4. 使用 30 天的保留期将数据提取到 Amazon Kinesis.使用 AWS Lambda 将数据记录写入 Amazon ElastiCache 以进行读取访问.

答案: B

解释:

B.最便宜并且可以胜任. D.最贵的一个.

Question 101

一家公司正在将业务关键型应用程序迁移到 AWS 上.它是使用 Oracle 数据库的传统三层 Web 应用程序. 数据在传输和静止时必须加密.该数据库承载 12 TB 的数据.允许通过内部网络与源 Oracle 数据库建立网

络连接,该公司希望通过使用 AWS 托管服务来降低运营成本.仅所有主键；但是,它包含许多二进制大对象(BLOB)字段.由于许可限制,无法使用数据库的本机复制工具.

哪种数据库迁移解决方案将对应用程序的可用性产生最小的影响?

1. 为 Amazon 实例设置 Amazon RDS.将 RDS 数据库托管在具有 Internet 访问权限的虚拟私有云(VPC) 子网中,并将 RDS 数据库设置为源数据库的加密只读副本.使用 SSL 加密两个数据库之间的连接.通过观察 RDS ReplicaLag 指标来监视复制性能.在应用程序维护窗口期间,在没有更多复制滞后时,请关闭本地数据库,并将应用程序连接切换到 RDS 实例.将只读副本提升为独立的数据库实例.
2. 设置一个 Amazon EC2 实例并安装相同的 Oracle 数据库软件.使用支持的工具创建源数据库的备份.在应用程序维护窗口期间,将备份还原到在 EC2 实例中运行的 Oracle 数据库中.设置一个

Amazon RDS for Oracle 实例,并在 AWS 托管的数据库之间创建导入作业. 作业完成后,关闭源数据库并将数据库连接切换到 RDS 实例.

1. 使用 AWS DMS 在本地 Oracle 数据库和 AWS 上托管的复制实例之间加载和复制数据集.设置启用了透明数据加密(TDE)的 Amazon RDS for Oracle 实例,并将其配置为复制实例的目标.创建一个客户管理的 AWS KMS 主密钥,将其设置为复制实例的加密密钥.

使用 AWS DMS 任务将数据加载到目标 RDS 实例中.在应用程序维护窗口期间以及加载任务到达正在进行的复制阶段之后,将数据库连接切换到新数据库.

1. 在应用程序维护窗口期间,在本地 Oracle 数据库上创建压缩的完整数据库备份.在执行备份时,提供 10 Gbps AWS Direct Connect 连接以提高数据库备份文件到 Amazon 的传输速度

S3,并缩短维护时段.使用 SSL / TLS 通过 Direct Connect 连接复制文件.成功复制备份文件后,请启动维护窗口,然后升高任何 Amazon RDS 支持的工具,以将数据导入启用了加密的新供应的 Oracle RDS for Oracle 实例.等待数据完全加载,然后将数据库连接切换到新数据库.删除 Direct Connect 连接以减少不必要的费用.

答案: C

解释:

1. 最佳解决方案,但不能使用本机复制B.备份可能不包含最新数据 C.您不能使用 KMS 密钥进行 TDE 加密,但是我们使用 KMS 对复制实例进行了加密,并将 TDE 用于新创建的 RDS 实例. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.ht ml https://docs.aws.amazon.com/dms/latest/userguide/CHAP\_Source.Oracle.html https://docs.aws.amazon.com/dms/latest/userguide/CHAP\_Target.SQLServer.html https://docs.aws.amazon.com/dms/latest/userguide/CHAP\_ReplicationInstance.htmlD.这将需要几个小 时迁移时

Question 102 **12/12考试原题**  **03/09考试原题**

一家公司检测到将一些工作负载转移到 AWS 上,以创建一个网格环境来运行市场分析.网格将由许多相似的实例组成,并通过作业计划功能启动.每次完成大型分析工作负载时,都会部署新的 VPC 以及作业调度程序和网格节点.多个网格可以并行运行.

关键要求是:

网格实例必须与 Amazon S3 通信以检索要处理的数据.

网格实例必须与 Amazon DynamoDB 通信以跟踪中间数据.作业调度程序仅需要与 Amazon EC2 API

通信以启动新的网格节点.

关键要求是环境无法直接或通过本地代理访问 Internet.但是,该应用程序需要能够与 Amazon S3,Amazon DynamoDB 和 Amazon EC2 API 无缝通信,而无需为每个新部署进行重新配置.

解决方案架构师应采取以下哪些措施来实现此目标体系结构? (选择三个.) A.为 Amazon S3 和 DynamoDB 启用 VPC 终端节点.

1. 禁用私有 DNS 名称支持.
2. 在网格实例上配置应用程序以使用 Amazon S3 终端节点的私有 DNS 名称. D.用 EC2 终结点的私有 IP 地址填充本地 DNS 服务器.
3. 为 EC2 启用接口 VPC 端点.
4. 将 Amazon S3 终端节点策略配置为仅允许从网格节点进行访问.

答案: ADE

解释:

A.https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html B.接口 VPC 端点需要专用DNS C.S3 端点是网关端点 s3 端点的私有 DNS 名称不是一个东西.您将需要对路由表使用前缀列表 ID, 并 继 续 对 服 务 使 用 S3 DNS 名 称 https://docs.aws.amazon.com/vpc/latest/userguide/vpce- gateway.html#vpc-endpoints -routing https://docs.aws.amazon.com/vpc/latest/userguide/vpc- endpoints-s3.htmlD.这是必需的,因为默认 EC2 端点路由仅填充在 VPC 路由表中,而专用 IP 用于接口端点 DNS 名称在 DNS 服务器中是必需的.

E. https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html F.S3 是网关端点,您不能在端点策略中限制主体

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-access.html#vpc-endpoint-policies

Question 103 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

对公司内部 AWS 资源的内部安全审核发现,许多运行 Microsoft Windows 工作负载的 Amazon EC2 实例缺少几个重要的操作系统级补丁.已要求解决方案架构师修复现有的修补程序缺陷,并开发工作流以确保识别并及时处理将来的修补程序要求.解决方案架构师已决定使用 AWS Systems Manager.重要的是,不要同时在所有 Windows 工作负载上重新启动 EC2 实例,以满足组织正常运行时间的要求.

哪个工作流程将自动满足这些要求?

1. 将具有 Windows Server 值的补丁程序组标记添加到所有现有 EC2 实例.确保为所有 Windows EC2 实例分配了该标签.将 AWS-DefaultPatchBaseline 与 Windows 服务器补丁程序组关联.定义一个 AWS Systems Manager 维护窗口,在其中进行修补,然后将其与 Windows Servers 修补程序组关联.使用关联的子网 ID 在维护窗口中注册实例.在每个维护窗口中将 AWS-RunPatchBaseline 文档分配为任务.
2. 向所有现有的 EC2 实例添加一个 Windows Server 值的补丁程序组标记.确保为所有 Windows EC2 实例分配了该标签.将 AWS-WindowsPatchBaseline 文档作为与 Windows Servers 修补程序组相关联的任务进行关联.创建一个 Amazon CloudWatch Events 规则,该规则配置为使用 cron 表达式来调度使用AWS Systems Manager run 命令执行修补的时间.创建一个 AWS Systems Manager 状态管理器文档,以定义要在补丁执行期间执行的命令.
3. 向所有现有的 EC2 实例添加一个值为 Windows Servers1 或 Windows Server2 的补丁程序组标记.确保为所有 Windows EC2 实例分配了该标签.关联 AWS-

具有两个 Windows Server 修补程序组的 DefaultPatchBaseline.定义两个不重叠的 AWS Systems Manager 维护窗口,在其中进行修补,然后将每个窗口与一个不同的修补程序组关联.使用补丁组标签在特定的维护窗口中注册目标.在每个维护窗口中将AWS-RunPatchBaseline 文档分配为任务.

1. 向所有现有的 EC2 实例添加一个值为 Windows server1 或 Windows Server2 的补丁程序组标记.确保为所有 Windows EC2 实例分配了该标签.关联 AWS-

具有两个 Windows Server 修补程序组的 WindowsPatchBaseline.定义两个不重叠的 AWS Systems Manager 维护窗口,在其中进行修补,然后将每个窗口与一个不同的修补程序组关联.在每个维护窗口中将AWS-RunWindowsPatchBaseline 文档分配为任务.创建一个 AWS Systems Manager 状态管理器文档, 以定义要在补丁执行期间执行的命令.

答案: C

解释:

A.所有实例都将在停机的同时进行修补 B.AWS-WindowsPatchBaseline 不是有效的修补实例.此外,在使用修补程序组时,不要使用 run 命令.

C.https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-scheduletasks.html https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman -patch-patchgroups.html D.AWS-WindowsPatchBaseline 无效

https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-baselines.html

Question 104 **12/12考试原题**  **03/09考试原题**

公司必须部署一个应用程序的多个独立实例.前端应用程序可以通过互联网访问.但是,公司政策规定,后端必须彼此隔离并与 Internet 隔离,但可以从集中式管理服务器进行访问.应用程序设置应该自动化,以最大程度地减少部署新实例时出现错误的机会.

哪个选项可以满足要求和最小化成本?

1. 使用 AWS CloudFormation 模板为每个区域创建相同的 IAM 角色.使用 AWS CloudFormation StackSets 通过使用针对每个实例进行自定义的参数来部署每个应用程序实例,并使用安全组隔离每个实例,同时允许访问中央服务器.
2. 使用 AWS CloudFormation StackSet 在单独的帐户中创建应用程序 IAM 角色和资源的每个实例.包括与管理中心服务器的 VPN 网关的 VPN 连接.
3. 使用单个 CloudFormation 模板在单独的帐户中复制应用程序 IAM 角色和资源.包括 VPC 对等连接,以将每个应用程序实例的 VPC 连接到中央 VPC.
4. 使用 AWS CloudFormation 模板的参数将部署自定义为单独的帐户.包括一个 NAT 网关,以允许通信回中央管理服务器.

答案: B

解释:

A.安全组不会应用于新创建的实例B.https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-vpn- gateway.html C.您不能使用单个 cloudformation 跨帐户 D.NAT 网关创建资源的模板将访问 Internet

Question 105 **12/12考试原题**  **03/09考试原题**

一组 Amazon EC2 实例已配置为高性能计算(HPC)集群.这些实例在一个放置组中运行,并且能够在高达

20 Gbps 的网络上相互通信.

集群需要与放置组外部的控制 EC2 实例进行通信.控制实例具有与其他实例相同的实例类型和 AMI,并配置有公共 IP 地址.

解决方案架构师如何提高控件实例与放置组中的实例之间的网络速度?

A.终止控件实例,然后在放置组中重新启动. B.确保实例正在使用专用 IP 地址进行通信. C.确保控件实例正在使用弹性网络适配器. D.将控件实例移到放置组中.

答案: D

解释:

HPC 已经与 ENA 一起运行,因为它已经具有高达 20 Gbps 的连接.我们需要做的就是将控件实例移到放置组中.另外,应该为支持的内核和实例类型自动启用 ENA,因此 C 是不正确的. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#change-instance- placement-group https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement -groups.html https://aws.amazon.com/blogs/aws/elastic-network-adapter-high-performance-network-interface-for- amazon-ec2/ https://docs.aws.amazon.com/ AWSEC2 / latest / UserGuide / enhanced-networking- ena.html

Question 106

解决方案架构师为三层应用程序创建了一个 AWS CloudFormation 模板,该模板包含运行自定义 AMI 的

Amazon EC2 实例的 Auto Scaling 组.

解决方案架构师希望通过首先更新模板以引用新的 AMI,然后调用 UpdateStack 将 EC2 实例替换为从新

AMI 启动的实例,来确保将来对自定义 AMI 的更新可以部署到正在运行的堆栈中. 如何部署 AMI 更新以满足这些要求?

1. 为模板的新版本创建一个更改集,查看对运行中的 EC2 实例的更改以确保 AMI 被正确更新,然后执行更改集.
2. 在模板中编辑 AWS :: AutoScaling :: LaunchConfiguration 资源,将其更改为 Replace.

删除政策

1. 在模板中编辑 AWS :: AutoScaling :: LaunchConfiguration 资源,插入属性.更新政策
2. 从更新的模板创建一个新的堆栈.成功部署后,修改 DNS 记录以指向新堆栈,然后删除旧堆栈.

答案: C

解释:

A.Old Instance 不会更新https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/update.stacks.walkthrough.html #update.walkthrough.ami B.DeletionPolicy 用于删除 https 后的行

为 ://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html C.https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-updatepolicy. html https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-as- launchconfig.html

Question 107 **12/12考试原题 03/23考题**

解决方案架构师正在设计一个具有 10 个现有帐户的多帐户结构.设计必须满足以下要求: 将所有帐户合并到一个组织中.

允许从主帐户和辅助帐户完全访问 Amazon EC2 服务.减少添加其他辅助帐户所需的精力. 解决方案中应包含哪些步骤组合? (选择两个.)

1. 从主帐户创建一个组织.将邀请从主帐户发送到辅助帐户.接受邀请并创建一个 OU.
2. 从主帐户创建一个组织.从每个辅助帐户向主帐户发送加入请求.接受请求并创建一个 OU. C.在主帐户和辅助帐户之间创建 VPC 对等连接.接受对 VPC 对等连接的请求.
3. 创建一个启用完全 EC2 访问的服务控制策略(SCP),并将该策略附加到 OU.
4. 创建一个完整的 EC2 访问策略,并将该策略映射到每个帐户中的一个角色.信任其他所有帐户以担任此角色.

答案: AD

解 释 : https://docs.aws.amazon.com/organizations/latest/userguide/orgs\_manage\_accounts\_invites.html

Question 108

在过去的几年中,AnyCompany 已收购了许多公司. AnyCompany 的 CIO 希望将每个被收购公司的资源分开存放.首席信息官还希望实施一种收费模式,在这种模式下,每个公司都要为其使用的 AWS 服务付费.

解决方案架构师负责设计一种 AWS 架构,该架构允许 AnyCompany 实现以下目标: 实施详细的退款机制,以确保每个公司都为其使用的资源付费.

AnyCompany 可以通过一张发票为所有公司支付AWS 服务的费用.

每个被收购公司的开发人员只能访问其公司中的资源.被收购公司的开发人员不应仅影响其公司的资源. 单个身份存储区用于对所有公司的开发人员进行身份验证.

以下哪种方法可以满足这些要求? (选择两个.)

A.使用每个公司的帐户创建一个多帐户策略.使用合并账单以确保AnyCompany 只需要支付一张账单. B.为每个公司创建一个带有虚拟私有云(VPC)的多帐户策略.通过不创建任何 VPC 对等链接来减少对公司的影响.由于所有内容都在一个帐户中,因此只有一张发票.使用标记为每个公司创建详细的帐单.

1. 为他们需要访问的帐户中的每个开发人员创建 IAM 用户.创建允许用户访问该帐户中所有资源的策略. 将策略附加到 IAM 用户.
2. 针对公司的 Active Directory 创建联合身份存储.创建具有适当权限的 IAM 角色,并设置与 AWS 和身份存储的信任关系.使用 AWS STS 授予用户基于身份存储中所属组的访问权限.
3. 使用每个公司的帐户创建一个多帐户策略.出于计费目的,请使用使用标签的标签解决方案来标识创建 每种资源的公司.

答案: AD

解释:

https://aws.amazon.com/blogs/security/how-to-set-up-uninterrupted-federated-user-access-to-aws- using- ad-fs/

Question 109 **12/12考试原题**  **03/09考试原题 03/23考题**

一家公司在两个区域(us-east-1 和 eu-west-1)中部署了三层 Web 应用程序.该应用程序必须同时在两个区域中都处于活动状态.该应用程序的数据库层在全球范围内使用单个 Amazon RDS Aurora 数据库,在us-east-1 中具有主数据库,在 eu-west-1 中具有只读副本.两个区域均通过 VPN 连接.

该公司希望确保即使在所有应用程序组件的区域级故障的情况下,该应用程序仍然可用.该应用程序处于 只读模式最多 1 小时是可以接受的.该公司计划配置两个 Amazon Route 53 记录集,每个区域一个.

公司应如何完成配置以满足其要求,同时为应用程序最终用户提供最低的延迟? (选择两个.)

答案: 使用故障转移路由并将 us-east-1 记录集配置为主,并将 eu-west-1 记录集配置为次.在 us-east-1 中为 Web 应用程序配置 HTTP 运行状况检查,并将其与 us-east-1 记录集相关联.

1. 使用加权路由,并将每个记录集的权重设置为 50.为每个区域配置 HTTP 运行状况检查,并将其附加到该区域的记录集.
2. 对两个记录集使用基于延迟的路由.为每个区域配置运行状况检查,并将其附加到该区域的记录集.
3. 为 us-east-1 中的运行状况检查配置 Amazon CloudWatch 警报,并使其调用 AWS Lambda 函数,该函数在 eu-west-1 中提升只读副本.
4. 通过调用在 eu-west-1 中提升只读副本的 AWS Lambda 函数,配置 Amazon RDS 事件通知以对 us- east-1 中的数据库故障做出反应.

答案: CE

解释:

A.这不能确保所有请求的延迟都短.B.不能保证低延迟 C.延迟路由还支持故障转移https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex- configs.html D.Healthy 检查失败并不意味着数据库失败

Question 110

一家公司在公共子网中运行 Windows Server 主机,该主机配置为允许一组管理员通过 RDP 连接以对专用子网中的主机的问题进行故障排除.主机必须始终在计划的维护时段之外可用,并且需要在发布后的 3 天内接收最新的操作系统更新.

用最少的管理努力来管理主机?

1. 在单实例 AWS Elastic Beanstalk 环境中运行主机.使用自定义 AMI 配置环境以使用 AWS Marketplace 中的强化机器映像.通过 AWS Systems Manager Patch Manager 应用系统更新.
2. 在 AWS WorkSpaces 上运行主机.使用 Amazon WorkSpaces 应用程序管理器(WAM)加固主机.将

Windows 自动更新配置为每 3 天进行一次.

1. 在最小和最大实例数为 1 的 Auto Scaling 组中运行主机.使用 AWS Marketplace 中的强化计算机映像. 通过 AWS Systems Manager Patch Manager 应用系统更新.
2. 在 AWS OpsWorks Stacks 中运行主机.在实例启动期间,使用 Chief 配方加固 AMI.

使用 AWS Lambda 计划的事件来运行"升级操作系统"堆栈命令以应用系统更新.

答案: B

解释:

A. 不 应 使 用 SSM 来 管 理 EB 实 例 . https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html

C.这可能有效,但是很难管理,因为实例可以被自动缩放组代替,并且 SMS 无法跟踪. D.upgrade 操作系统仅适用于 Linux

https://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks-commands.html

Question 111

一家公司拥有一个大型的本地 Apache Hadoop 群集,其中包含 20 PB HDFS 数据库.群集每季度增长大约 200 个实例和 1 PB.该公司的目标是实现其 Hadoop 数据的弹性,限制丢失群集节点的影响并显着降低成本.当前的群集运行 24/7,并支持各种分析工作负载,包括交互式查询和批处理.

哪种解决方案能以最少的花费和最少的时间满足这些要求?

1. 使用 AWS Snowmobile 将现有群集数据迁移到 Amazon S3.创建持久性 Amazon EMR 集群,该集群最初的大小应根据本地集群中的历史数据来处理交互式工作负载.将数据存储在 EMRFS 上.使用针对主节点和核心节点的预留实例以及针对任务节点的竞价型实例,并根据 Amazon CloudWatch 指标自动扩展任务节点,以最大程度地降低成本.为类似优化的批处理工作负载创建特定于作业的优化集群.
2. 使用 AWS Snowmobile 将现有群集数据迁移到 Amazon S3.创建一个持久性 Amazon EMR 集群,其大小和配置与当前集群相似.将数据存储在EMRFS 上.通过使用预留实例将成本降至最低.随着工作负载每季度增加,请购买其他预留实例并添加到群集中.
3. 使用 AWS Snowball 将现有群集数据迁移到 Amazon S3.创建持久性 Amazon EMR 集群,该集群最初的大小应根据本地集群中的历史数据来处理交互式工作负载.将其存储在 EMRFS 上.使用针对主节点和核心节点的预留实例以及针对任务节点的竞价型实例,并根据Amazon CloudWatch 指标自动扩展任务节点,以最大程度地降低成本.为类似优化的批处理工作负载创建特定于作业的优化集群.
4. 使用 AWS Direct Connect 将现有群集数据迁移到 Amazon S3.创建持久性 Amazon EMR 集群,该集群最初的大小应根据本地集群中的历史数据来处理交互式工作负载.将数据存储在 EMRFS 上.使用针对主节点和核心节点的预留实例以及针对任务节点的竞价型实例,并根据Amazon CloudWatch 指标自动扩展任务节点,以最大程度地降低成本.为类似优化的批处理工作负载创建特定于作业的优化集群.

答案: A

解释:

B.每季度购买额外的 RI 将无法通过交互式查询和批处理来自动扩展 C.AWS 建议使用 Snowmobile 来存储大于 10PB 的数据 D.直接连接将花费数年

Question 112 **12/12考试原题**  **03/09考试原题**

公司正在内部运行大型应用程序.它的技术堆栈包括用于 Web 服务器平台的 Microsoft .NET 和用于数据库的 Apache Cassandra.该公司希望将应用程序迁移到 AWS 以提高服务可靠性. IT 团队还希望减少花费在容量管理和维护该基础架构上的时间.开发团队愿意并随时进行代码更改以支持迁移.

迁移后,至少要管理哪种设计?

1. 将 Web 服务器迁移到运行.NET 的 Auto Scaling 组中的 Amazon EC2 实例.使用多个只读副本将现有的 Cassandra 数据库迁移到 Amazon Aurora,并以多可用区模式运行两者.
2. 将 Web 服务器迁移到在 Multi-AZ Auto Scaling 配置中运行.NET 平台的 AWS Elastic Beanstalk 环境. 将 Cassandra 数据库迁移到以多可用区配置运行的 Amazon EC2 实例.
3. 将 Web 服务器迁移到在 Multi-AZ Auto Scaling 配置中运行.NET 平台的 AWS Elastic Beanstalk 环境. 将现有的 Cassandra 数据库迁移到 Amazon DynamoDB.
4. 将 Web 服务器迁移到运行.NET 的 Auto Scaling 组中的 Amazon EC2 实例.将现有的 Cassandra 数据库迁移到 Amazon DynamoDB.

答案: C

解释:

* 1. C2 B.EC2 数据库不好 D.EC2 管理成本更高

Question 113 **11/19考试原题**

公司有一项要求,即仅允许将经过特殊加固的 AMI 启动到 VPC 中的公共子网中,并且将 AMI 与特定的安全组关联.如果允许不符合要求的实例运行到公共子网中,则可能会带来重大的安全风险.

同一 AWS 账户的 Amazon DynamoDB 表中存在批准的 AMI,子网到安全组的映射.该公司创建了一个AWS Lambda 函数,如果在 DynamoDB 表中未批准 AMI,子网和安全组的组合,则该函数将在调用时终止给定的 Amazon EC2 实例.

解决方案架构师应如何对 MOST 进行快速缓解合规性偏离的风险?

1. 创建一个 Amazon CloudWatch Events 规则,该规则与每次使用允许的 AMI 之一启动 EC2 实例时匹配, 并将其与 Lambda 函数关联为目标.
2. 对于接收 Aws CloudTrail 日志的 Amazon S3 存储桶,创建带有过滤器的 S3 事件通知配置,以在日志包含 ec2:RunInstances 操作时进行匹配,并将其与作为目标的 Lambda 函数相关联.
3. 启用 AWS CloudTrail 并将其配置为流式传输到 Amazon CloudWatch Logs 组.在 CloudWatch 中创建指标筛选器以匹配 ec2:RunInstances 操作何时发生,并在指标大于 0 时触发Lambda 函数.
4. 创建一个每次启动 EC2 实例时都匹配的 Amazon CloudWatch Events 规则,并将其与作为目标的

Lambda 函数相关联

答案: D

解释:

A.不会停止不合规启动的 AMI B.Cloudtrail 日志最多可以显示 5 到 15 分钟,以显示https://docs.aws.amazon.com/awscloudtrail/latest/userguide/get-and-view-cloudtrail-log- files.html C.Cloudtrail 可以监视 ec2:Runinstance api 调用,但是 Cloudtrail 日志最多可以显示 5 到 15 分钟才能显示 https://docs.aws.amazon.com/AWSEC2/latest/APIReference/using-cloudtrail.html

Question 114 **12/12考试原题**  **03/09考试原题**

解决方案架构师必须迁移具有 70 TB 静态文件的现有本地Web 应用程序,以支持公共开放数据计划.架构师希望升级到主机操作系统的最新版本,这是迁移工作的一部分.

哪种和最快,最经济的方式来执行迁移?

1. 在应用程序服务器上运行从物理到虚拟的转换.通过互联网传输服务器映像,然后将静态数据传输到Amazon S3.
2. 在应用程序服务器上运行从物理到虚拟的转换.通过 AWS Direct Connect 传输服务器映像,并将静态数据传输到 Amazon S3.
3. 将服务器重新平台到 Amazon EC2,然后使用 AWS Snowball 将静态数据传输到 Amazon S3.
4. 通过使用 AWS Server Migration Service 将代码和数据移动到新的 Amazon EC2 实例来重新平台化服务器.

答案: C

解释:

A. 服 务 器 迁 移 服 务 不 支 持 P2V, 而 EC2 https://forums.aws.amazon.com/thread.jspa?messageID=794316&tstart=0 https://docs.aws.amazon.com/server-migration-service/latest/userguide/prereqs.html 服务器迁移服务不支持 B.P2V D.SMS 无法更新操作系统

Question 115 **12/12考试原题** **11/19考试原题 03/23考题**

一家公司拥有一个应用程序,该应用程序生成的天气预报每 15 分钟更新一次,输出分辨率为 10 亿个唯一

位置,每个位置的大小约为 20 个字节(每个预测 20 GB).每小时,全球将访问预测数据约 500 万次(每秒

1400 个请求),在天气事件期间,访问量最多可增长 10 倍.每次更新都会覆盖预测数据.当前天气预报应用程序的用户希望对查询的响应将在不到两秒钟的时间内返回给每个请求.

哪种设计满足要求的请求率和响应时间?

1. 将预测位置存储在 Amazon ES 集群中.使用以 Amazon Lambda 函数为响应源的查询作为目标的Amazon API Gateway 终端节点的 Amazon CloudFront 分配.在 API 网关阶段启用 API 缓存,并将缓存控制超时设置为 15 分钟.
2. 将预测位置存储在 Amazon EFS 卷中.创建一个 Amazon CloudFront 发行版,该发行版的目标是已安装Amazon EFS 卷的 Amazon EC2 实例的 Auto Scaling 机队的 Elastic Load Balancing 组.在 CloudFront 分配中将设置的缓存控制超时设置为 15 分钟.
3. 将预测位置存储在 Amazon ES 集群中.使用针对具有 AWS Lambda 函数的 API 网关终端节点的Amazon CloudFront 分发,该 AWS Lambda 函数以查询为源进行响应.创建一个 Amazon Lambda @ Edge 函数,该函数在边缘位置本地缓存数据 15 分钟.
4. 将预测位置作为单个对象存储在 Amazon S3 中.创建一个针对 EC2 实例的 Auto Scaling 机群的Elastic Load Balancing 组的 Amazon CloudFront 分配,查询 S3 对象的来源.在 3CloudFront 发行版中将缓存控制超时设置为 15 分钟.

答案: A

解释:

1. API 网关缓存将在API 网关的区域中https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html 此外,API 网关具有请求限制https://docs.aws.amazon.com/apigateway/latest/developerguide/limits.html
2. 缓存控制标头设置在原始位置,而不是云端https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html
3. 不需要 Lambda @ Edge 进行 Cloudfront 缓存,但是您可以将数据缓存在 Lambda 内存中.但是,对于20GB 的数据,这将太多了..由于您还使用 Lambda @ Edge 进行缓存,因此命中率很可能会超过并发限制https://aws.amazon.com/blogs/networking-and-content-delivery/leveraging-external-data-in- lambdaedgehttps://aws.amazon.com/blogs/networking-and-content-delivery/lambdaedge- design- best-practices / D.Cache-control 标头设置在原始位置,而不是在 Cloudfront 中https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html

Question 116

一家公司正在使用 AWS CloudFormation 部署其基础架构.该公司担心,如果删除生产 CloudFormation 堆栈,则可能还会删除存储在 Amazon RDS 数据库或 Amazon EBS 卷中的重要数据.

公司如何防止用户以这种方式意外删除数据?

1. 修改 CloudFormation 模板,以将 DeletionPolicy 属性添加到 R DS 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 策略以拒绝删除带有标签的 RDS 和 EBS 资源. " aws:cloudformation:stackname"
4. 使用 AWS Config 规则来防止删除 RDS 和 EBS 资源.

答案: A

解释:

1. https://aws.amazon.com/premiumsupport/knowledge-center/delete-cf-stack-retain-resources/ B.更新堆栈时使用堆栈策略

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.htmlC.

这将防止故意删除 D.Config 规则用于监视而非预防

Question 117 **11/19考试原题**

一家公司希望通过使用 Amazon API Gateway 实施无服务器应用程序,

AWS Lambda 和 Amazon DynamoDB.他们部署了概念证明,并指出平均响应时间大于其上游服务可以接受的 Amazon CloudWatch 指标,这并不表示 DynamoDB 出现任何问题,但表明某些 Lambda 功能正在超时.

解决方案架构师应考虑采取以下哪些行动来提高性能? (选择两个.) A.配置 AWS Lambda 函数以重用容器,以避免不必要的启动时间.

1. 增加内存量并调整 Lambda 函数的超时.进行完整的性能测试,以确定 Lambda 函数的理想内存和超时

配置.

1. 创建一个运行 Memcached 的 Amazon ElastiCache 集群,并配置 Lambda 函数以进行 VPC 集成并访问 Amazon ElastiCache 集群.
2. 在 Amazon API Gateway 的适当阶段启用 API 缓存,并为需要比整个阶段 TTL 更低的单个方法覆盖

TTL.

答案: BD

解释:

A.没有这样的东西,这是自动的 C.这没有多大帮助

Question 118 **11/19考试原题**  **03/09考试原题 03/23考题**

一家公司正在使用 AWS 运行以 Node.js 编写的面向互联网的生产应用程序.开发团队负责将其软件的新版本直接推向生产环境.每天多次更新应用程序软件.团队需要解决方案架构师的指导,以帮助他们将软件快速部署到生产团队中,并且对服务的中断最少.

哪个选项满足这些要求?

1. 将软件预打包到 AMI 中,然后使用 Auto Scaling 部署生产团队.对于软件更改,请更新 AMI 并允许 Auto Scaling 将新 AMI 自动推入生产环境.
2. 使用 AWS CodeDeploy 将预打包的 AMI 推入生产环境.对于软件更改,请使用新的 AMI 标识重新配置

CodeDeploy,以将新的 AMI 推入生产团队.

1. 使用 AWS Elastic Beanstalk 托管生产应用程序.对于软件更改,请将新的应用程序版本上载到 Elastic Beanstalk,以使用蓝/绿部署方法将其推送到生产团队.
2. 通过 Auto Scaling 部署基础 AMI,并使用用户数据引导软件.对于软件更改,请使用 SSH 到每个实例,然后用新版本替换软件.

答案: C

解释:

A.AMI 应该是基线 B.CodeDeploy 无法部署 AMI C.Manaul 工作

Question 119

一家公司使用 Amazon EC2 实例来部署 Web 队列来托管博客网站. EC2 实例位于应用程序负载平衡器(ALB)的后面,并在 Auto Scaling 组中进行配置.该 Web 应用程序将所有博客内容存储在 Amazon EFS 卷上.

该公司最近为博客作者添加了一项功能,可将视频添加到他们的帖子中,吸引的访问量是以前的 10 倍.在一天中的高峰时段,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.

哪种 MOST 具有成本效益和可伸缩性的部署可以为用户解决问题? A.重新配置 Amazon EFS 以启用最大 I / O.

1. 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中,在关机时将站点内容复制 到 Amazon S3 中.
2. 配置一个 Amazon CloudFront 分配.将发行版指向S3 存储桶,然后将视频从 EFS 迁移到 Amazon S3. D.为所有套件内容设置一个 Amazon CloudFront 分配,并将该分配指向 ALB.

答案: C

解释:

A.对 EC2 可能没有太大帮助,可能是瓶颈 B.事故发生时数据丢失 D.仍然使用 EC2 服务

Question 120 **12/12考试原题**  **03/09考试原题**

一家公司在 Amazon ECS 上运行其容器化批处理作业.通过将容器映像,任务定义和相关数据提交到Amazon S3 存储桶来调度作业.每个作业的容器映像可能是唯一的.尽快运行作业至关重要,因此将作业工件提交到 S3 存储桶会触发作业立即运行.有时可能根本没有作业在运行.但是,任何大小的作业都可以在没有警告的情况下提交给 IT 运营团队.作业定义包括 CPU 和内存资源要求.

什么样的解决方案将使批处理作业在计划后尽快完成?

1. 使用 Amazon EC2 启动类型在 Amazon ECS 集群上计划作业.使用服务自动缩放可增加或减少正在运行的任务数,以适合正在运行的作业数.
2. 直接在 EC2 实例上计划作业.将预留实例用于基线的最小负载,并在 Auto Scaling 组中使用按需实例以根据需求扩展平台.
3. 使用 Fargate 启动类型在 Amazon ECS 集群上计划作业.使用服务自动缩放可增加或减少正在运行的任务数,以适合正在运行的作业数.
4. 使用 Fargate 启动类型计划 Amazon ECS 集群上的作业.在 Auto Scaling 组中使用竞价型实例可根据需求扩展平台.使用服务自动缩放可增加或减少正在运行的任务数,以适合正在运行的作业数.

答案: C

解释:

A.EC2 大小将是作业资源的限制.B.EC2 大小将是作业资源的限制.同样,我们无法确定基准,因为可以提交任何大小的作业 C.由于可以立即启动作业并且可以运行不受 EC2 大小限制的 D,因此可以选择Fargate.Fargate 与 EC2 大小无关竞价型实例,在请求时竞价型实例也可能不可用

Question 121 **12/12考试原题**  **03/09考试原题 03/23考题**

公司每五分钟将点击流数据文件接收到 Amazon S3. Python 脚本每天在 Amazon EC2 实例上作为 cron 作业运行,以处理每个文件并将其加载到 Amazon RDS 上托管的数据库中. cron 作业需要 15 到 30 分钟才能处理 24 小时的数据.数据使用者要求尽快提供数据.

哪种解决方案可以达到预期的结果?

1. 增加实例的大小以加快处理速度,并更新计划以每小时运行一次.
2. 将 cron 作业转换为 AWS Lambda 函数,并在 EC2 实例上使用 cron 作业触发此新功能.
3. 将 cron 作业转换为 AWS Lambda 函数,并使用 Amazon CloudWatch 事件将其安排为每小时运行一次.
4. 创建一个 AWS Lambda 函数,该函数在使用S3 事件通知将文件传递到 Amazon S3 时运行. 答案: D

Question 122

一家不熟悉 AWS 的公司报告说,它已经耗尽了基本支持计划中多个帐户的服务限制.该公司希望防止将来发生这种情况.

监视和管理公司帐户中所有服务限制的最有效的方法是什么?

1. 使用 Amazon CloudWatch 和 AWS Lambda 通过 AWS Trusted Advisor 定期计算所有链接账户的限额,如果限额接近阈值,则使用 Amazon SNS 提供通知.
2. 寻求 AWS 支持以主动提高所有账户的限额.这样,客户避免了仅仅为了提高服务限制而创建和管理基础结构.
3. 使用 Amazon CloudWatch 和 AWS Lambda 通过 AWS Trusted Advisor 定期计算所有链接帐户的限制,以编程方式增加接近阈值的限制.
4. 使用 Amazon CloudWatch 和 AWS Lambda 使用 AWS Trusted Advisor 定期计算所有链接帐户的限制,如果限制接近阈值,则使用 Amazon SNS 进行通知.确保账户至少使用 AWS 业务支持计划.

答案: D

解释:

要将服务限制与 cloudwatch 一起使用,您将需要业务计划 https://aws.amazon.com/about-aws/whats- new/2017/11/aws-trusted-advisor-adds-service-limit-dashboard- and-cloudwatch -metrics / https://aws.amazon.com/blogs/mt/monitoring-service-limits-with-trusted-advisor-and-amazon- cloudwatch/

Question 123  **03/09考试原题**

公司需要运行具有许可证的软件包,该许可证必须在使用期间在同一物理主机上运行.该软件包仅可使用

90 天.该公司要求每 30 天修补并重新启动所有实例. 使用 AWS 如何满足这些要求?

1. 运行一个专用实例,禁用自动放置.
2. 在主机关联性设置为主机的专用主机上运行实例. C.运行带有预留实例的按需实例以确保一致的放置. D.在终止设置为 90 天的许可主机上运行实例.

答案: B

解释:

A.自动放置是专用主机而非专用实例的设置,并且您不能保证重启后将实例部署到同一主机B.https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how- private-hosts-work.html C.最好的办法是保留在 AZ 中,而不是硬件中..D.这是错误的.

Question 124  **03/09考试原题 03/23考题**

一家公司在 AWS 上运行 IoT 平台.各地的 IoT 传感器将数据发送到在 Application Load Balancer 后面运行的 Amazon EC2 实例上公司的Node.js API 服务器.数据存储在使用 4 TB 常规数据的 Amazon RDS MySQL 数据库实例中

用途 SSD 卷.公司在现场部署的传感器数量

随着时间的流逝而增加,并且有望显着增长. API 服务器始终过载,RDS 指标显示高写入延迟.

以下哪些步骤可以共同解决问题,并能在配置新传感器时实现增长,同时保持该平台的成本效益? (选择两个.)

1. 将 MySQL 通用 SSD 存储器的大小调整为 6 TB,以提高该卷的 IOPS
2. 重新架构数据库层以使用 Amazon Aurora 代替 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. 重新架构数据库层以使用 Amazon DynamoDB 代替 RDS MySQL 数据库实例

答案: CE

解释:

A.将大小调整为 6TB 会将 IOPS 性能从 12288 更改为 16000,但是 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.Aurora 理论上应该没有 IOPS 问题,但是它的最大大小限制仍然是64TB C.像这样的流非常适合数据处理 D.Dynamo 没有最大数据大小限制,这很适合

Question 125

解决方案架构师正在设计一个系统,该系统将从 2000 个联网传感器收集和存储数据.每个传感器每秒产生

1 KB 数据.数据必须在发送到系统并无限期存储用于分析的几秒钟内可供分析. 哪个是收集和存储数据的最具成本效益的解决方案?

1. 将每个记录放入 Amazon Kinesis Data Streams 中.使用 AWS Lambda 函数将每个记录写入带有前缀的 Amazon S3 中的对象,该前缀按小时组织记录并哈希记录的键.分析 Kinesis Data Streams 中的最新数据和 Amazon S3 中的历史数据.
2. 将每个记录放入 Amazon Kinesis Data Streams 中.设置 Amazon Kinesis Data Firehouse 以从流中读取记录并将它们分组为 Amazon S3 中的对象.分析 Kinesis Data Streams 中的最新数据和 Amazon S3 中的历史数据.
3. 将每条记录放入 Amazon DynamoDB 表中.通过查询表来分析最近的数据.使用连接到 DynamoDB 流的 AWS Lambda 函数将记录分组在一起,将它们写入 Amazon S3 中的对象,然后从 DynamoDB 表中删除记录.分析 DynamoDB 表中的最新数据和 Amazon S3 中的历史数据
4. 将每个记录放入带有前缀的 Amazon S3 中的对象中,该前缀按小时组织记录并哈希记录的键.使用 S3 生命周期管理将对象过渡到 S3 频繁访问存储,以降低存储成本.通过访问 Amazon S3 中的数据来分析最新数据和历史数据

答案: A

解释:

B.我们可以使用 kinesis firehose 数据转换进行分组,但是答案没有提及,因此无法分组.此外,firehose 的价格可能会很高,因为它至少要收取 5 KB 的费用https://docs.aws.amazon.com/firehose/latest/dev/data- transformation.html C.将流 D 与记录分组非常困难.由于 S3 IA 的最低计费大小为 128 KB,因此不会有太大帮助

Question 126 **11/19考试原题 03/23考题**

拍卖网站使用户可以对收藏品进行竞标.拍卖规则要求每个出价只能按接收到的顺序处理一次.当前实施 基于一系列 Amazon EC2 Web 服务器,这些服务器将出价记录写入 Amazon Kinesis Data Streams.

一个 t2.large 实例具有一个 cron 作业,该作业运行出价处理器,该处理器从 Kinesis Data Streams 读取传入的出价并处理每个出价.拍卖网站越来越受欢迎,但用户抱怨有些出价没有注册.

故障诊断表明出价处理器在需求高峰时段过慢,有时在处理过程中崩溃,并有时无法跟踪正在处理的记录. 哪些更改应该使投标处理更加可靠?

1. 将出价发布到 Kinesis Data Streams 时,重构 Web 应用程序以使用 Amazon Kinesis Producer 库(KPL).重构出价处理器,以将 Kinesis 数据流中的每条记录标记为未读,处理和处理.在每次投标处理运行开始时,扫描 Kinesis 数据流以查找未处理的记录.
2. 重构 Web 应用程序,以将每个传入的出价发布到 Amazon SNS 主题上,代替 Kinesis Data Streams.配置 SNS 主题以触发 AWS Lambda 函数,该函数会在用户提交出价后立即对其进行处理.
3. 重构 Web 应用程序,以将每个传入的出价发布到Amazon SQS FIFO 队列中,以代替 Kinesis Data Streams.重构投标处理器以连续地 SQS 队列.将出价处理 EC2 实例放置在 Auto Scaling 组中,最小和最大大小为 1.
4. 将 EC2 实例类型从 t2.large 切换为更大的常规计算实例类型.根据 Kinesis 数据流中的IncomingRecords 指标,将出价处理器 EC2 实例放入一个 Auto Scaling 组中,该组可以扩展运行出价处理器的 EC2 实例的数量.

答案: C

解释:

AI 认为您不能在 Kinesis B 中标记记录.Lambda 具有并发限制,SNS 无法保证订单 C.不可扩展,但这是此处的最佳答案.对于 FIFO 队列,我们 实际上可以有多个使用者并且使用消息组 ID . D.Scaling 可能会有所帮助,但是出价处理器可能仍然崩溃,并且仍然不能保证出价已被处理. (Kinesis 没有消息级别的确认/失败)

Question 127  **03/09考试原题**

一家公司已要求解决方案架构师设计一种安全的内容管理解决方案,外部客户应用程序可以通过API 调用对其进行访问.该公司要求客户管理员必须能够提交 API 调用,并根据需要回滚对发送到内容管理解决方案的现有文件的更改.

满足所有解决方案要求的 MOST 安全部署设计是什么?

1. 将 Amazon S3 用于对象存储,同时启用版本控制和存储桶访问日志记录,以及每个客户应用程序的 IAM 角色和访问策略.使用 SSE-KMS 加密对象.开发内容管理应用程序以为每个客户使用单独的 AWS KMS 密钥.
2. 使用 Amazon WorkDocs 进行对象存储.利用 WorkDocs 加密,用户访问管理和版本控制.使用 AWS CloudTrail 记录所有 SDK 操作并通过 Amazon CloudWatch 仪表板创建按小时访问的报告.基于静态Amazon S3 网页在 SDK 中启用还原功能,该网页显示 CloudWatch 仪表板的输出.
3. 使用 Amazon EFS 进行对象存储,对 Amazon EFS 卷使用静态加密,并使用 AWS KMS 中存储的客户托管密钥.使用 IAM 角色和 Amazon EFS 访问策略为每个客户应用程序指定单独的加密密钥.部署内容管理应用程序,以将所有新版本作为新文件存储在Amazon EFS 中,并使用控件 API 将特定文件还原为先前版本.
4. 使用 Amazon S3 通过版本控制存储对象,并启用 S3 存储桶访问日志记录.对每个客户应用程序使用IAM 角色和访问策略.使用客户端加密对对象进行加密,并在访问内容管理应用程序时将加密密钥分发给所有客户.

答案: A

解释:

1. 可以.使用 HTTPS,我们甚至可以在传输过程中进行加密.您可以在 S3 请求标头上指定密钥. https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPUT.html B.WorkDocs 确实不是为此设计的. C.您可以为 EFS 指定加密密钥,但是应该使用 KMS 完成政策. EFS 访问策略用于控制诸如管理

访问,而不是文件访问之类的操作https://docs.aws.amazon.com/efs/latest/ug/efs-api-permissions- ref.html D.将密钥交付给客户端不是非常安全.

第 128 题

一家公司一直在使用第三方提供商作为其内容交付网络,并且最近决定切换到 Amazon CloudFront,开发团队希望最大限度地提高全球用户群的性能.该公司使用的内容管理系统(CMS)可以提供静态和动态内容. CMS 均是应用程序负载平衡器(ALB),它被设置为分发的默认来源.

静态资产从 Amazon S3 存储桶提供.原始访问身份(OAI)已创建,并且 S3 存储桶策略已更新为允许来自

OAI 的 GetObject 操作,但是静态资产收到 404 错误.

解决方案架构师应采取哪些步骤来纠正错误? (选择两个.) A.将另一个来源添加到 CloudFront 分配中以获取静态资产

1. 将基于路径的规则添加到 ALB 以转发对静态资产的请求
2. 添加一个 RTMP 发行版以允许缓存静态和动态内容
3. 将行为添加到 CloudFront 分配中以获取路径模式和静态资产的来源
4. 将主机标头条件添加到 ALB 侦听器,并从 CloudFront 转发标头以将流量添加到允许列表答案: AD

Question 129  **03/09考试原题**

一家银行将其基于大型机的信用卡批准处理应用程序重新架构为 AWS 云上的云原生应用程序.

在峰值负载下,新应用程序每秒将接收多达 1,000 个请求.每个事务有多个步骤,并且每个步骤都必须接收

上一步的结果.整个请求必须在不到 2 秒的时间内返回授权响应,且数据丢失为零.每个请求都必须收到响应.该解决方案必须符合支付卡行业数据安全标准(PCI DSS).

哪一种选择能够以最低的复杂度和最低的成本满足银行的所有目标,同时又满足合规性要求?

1. 使用一个 AWS Lambda 任务创建一个 Amazon API Gateway 来处理入站请求,该任务执行多个步骤并返回具有批准状态的 JSON 对象.打开一个支持案例以增加并发 Lambda 数的限制,以便为由于新应用程序而导致的突发事件腾出空间.
2. 在目标组中的 Amazon EC2 专用实例上创建具有 Amazon ECS 集群的 Application Load Balancer,以处理传入请求.使用 Auto Scaling 可根据平均 CPU 使用率来扩展/扩展群集.部署处理所有批准步骤并返回带有批准状态的 JSON 对象的 Web 服务.
3. 在专用实例上的 Amazon EC2 上部署应用程序.在 Auto Scaling 组中的应用程序服务器场前面使用Elastic Load Balancer 来处理传入的请求.在测量单个实例的容量之后,基于自定义 Amazon CloudWatch 指标针对每秒入站请求数进行横向扩展/扩展.
4. 创建一个 Amazon API Gateway,以使用一系列 AWS Lambda 流程处理入站请求,每个流程都有一个Amazon SQS 输入队列.每一步骤完成时,它将结果写入下一步骤的队列.最后一步返回带有批准状态的JSON 对象.打开一个支持案例以增加并发 Lambda 数的限制,以便为由于新应用程序而导致的突发事件腾出空间.

答案: D

解释:

这是唯一保证 0 数据丢失的设备

Question 130

解决方案架构师正在将 10 TB PostgreSQL 数据库迁移到Amazon RDS,用于

PostgreSQL.该公司的 Internet 链接为 50 MB,在 Amazon VPC 中具有VPN,并且解决方案架构师需要在过渡之前迁移数据并同步更改.

转换必须在 8 天之内进行.

安全可靠地迁移数据库的最小复杂方法是 什么?

1. 订购一个 AWS Snowball 设备并使用 AWS DMS 复制数据库.当数据库在 Amazon 3 中可用时,请使用

AWS DMS 将其加载到 Amazon RDS,并配置作业以在转换之前同步更改.

1. 创建一个 AWS DMS 作业以将数据从本地连续复制到 AWS.数据同步后切换到 Amazon RDS.
2. 订购一个 AWS Snowball 设备并将数据库转储复制到该设备.将数据复制到 Amazon S3 之后,将其导入到 Amazon RDS 实例.设置 VPN 上的日志传送,以在切换前同步更改.
3. 订购一个 AWS Snowball 设备并使用 AWS Schema Conversion Tool 复制数据库.

当数据在 Amazon S3 中可用时,请使用AWS DMS 将其加载到 Amazon RDS,并配置作业以在转换之前同步更改.

答案: D

解释:

互联网连接可能需要 8 天以上的时间才能迁移

https://docs.aws.amazon.com/dms/latest/userguide/CHAP\_LargeDBs.html

Question 131 **11/19考试原题 03/23考题**

解决方案架构师必须使用蓝/绿部署方法来更新 AWS Elastic Beanstalk 中的应用程序环境.解决方案架构师创建与现有应用程序环境相同的环境,并将该应用程序部署到新环境.

接下来应该怎么做才能完成更新?

1. 使用 Amazon Route 53 重定向到新环境
2. 选择交换环境 URL 选项
3. 替换 Auto Scaling 启动配置
4. 更新 DNS 记录以指向绿色环境

答案: B

解释:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html

Question 132 **11/19考试原题 03/23考题**

公司的旧版应用程序在内部服务器上运行.增加

应用程序的可靠性,该公司希望使用应用程序日志获得可行的见解. 已为解决方案架构师提供了以下解决方案要求:

-使用 AWS 聚合日志.

-自动日志分析错误.

-当错误超出规定范围时通知运营团队阈.

哪种解决方案符合要求?

1. 在服务器上安装 Amazon Kinesis Agent,将日志发送到 Amazon Kinesis Data Streams,并使用Amazon Kinesis Data Analytics 识别错误,创建 Amazon CloudWatch 警报以通知操作团队错误
2. 在服务器上安装 AWS X-Ray 代理,将日志发送到 AWS Lambda 并进行分析以识别错误,然后使用

Amazon CloudWatch Events 通知操作团队错误.

1. 在服务器上安装 Logstash,将日志发送到 Amazon S3,然后使用 Amazon Athena 识别错误,使用

sendmail 通知操作团队错误.

1. 在服务器上安装 Amazon CloudWatch 代理,将日志发送到 Amazon CloudWatch Logs,并使用指标过滤器识别错误,创建 CloudWatch 警报以将错误通知运维团队.

答案: D

解释:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on- 前 提.html

Question 133 **12/12考试原题**

解决方案架构师可以采取哪些步骤组合来保护在 Amazon EC2 上运行的 Web 工作负载免受 DDoS 和应用程序层攻击? (选择两个.)

1. 将 EC2 实例放在网络负载均衡器后面,并在其上配置AWS WAF.
2. 将 DNS 迁移到 Amazon Route 53 并使用 AWS Shield.
3. 将 EC2 实例放入 Auto Scaling 组中,并在其上配置 AWS WAF.
4. 创建并使用 Amazon CloudFront 发行版,并在其上配置 AWS WAF.
5. 在 VPC 中创建和使用 Internet 网关,然后使用 AWS Shield.

答案: BD

解释:

1. https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/
2. WAF 不适用于自动秤组https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html 打 击 文 档 中 提 到 了 Cloudfront,Route 53,AWS Shield 和 WAF https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/

Question 134 **12/12考试原题**  **03/09考试原题**

一家照片共享和出版公司每天接收 10,000 至 150,000 张图像.公司从多个注册了该服务的供应商和用户处接收图像.该公司正在迁移到 AWS,并希望通过使用 Amazon Rekognition 添加数据来丰富现有元数据. 以下是其他数据的示例:

作为云迁移计划的一部分,该公司将现有图像数据上传到 Amazon S3,并告诉用户直接将图像上传到Amazon S3.解决方案架构师应怎么做才能满足这些要求?

1. 根据 S3 事件通知触发 AWS Lambda,以使用Amazon Rekognition 创建其他元数据.使用 Amazon DynamoDB 存储元数据,然后使用 Amazon ES 创建索引.使用 Web 前端提供由 Amazon ES 支持的搜索功能.
2. 使用 Amazon Kinesis 基于 S3 事件流数据.使用在Amazon EC2 中运行的应用程序从图像中提取元数据.然后将数据存储在 Amazon DynamoDB 和 Amazon CloudSearch 上并创建索引.使用具有CloudSearch 支持的搜索功能的 Web 前端.
3. 根据 S3 事件通知启动 Amazon SQS 队列.然后让 Amazon SQS 将元数据信息发送到 Amazon DynamoDB.在 Amazon EC2 上运行的应用程序使用 API 从 Amazon Rekognition 提取数据,并将数据添加到 DynamoDB 和 Amazon ES.使用 Web 前端提供由 Amazon ES 支持的搜索功能.
4. 根据 S3 事件通知触发 AWS Lambda,以使用 Amazon Rekognition 创建其他元数据.使用 Amazon RDS MySQL Multi-AZ 来存储元数据信息,并使用 Lambda 创建索引.使用具有 Lambda 支持的搜索功能的 Web 前端.

答案: A

解释:

B. Kinesis 无法直接从 S3 事件中流式传输数据,而 EC2 本身并不是最佳的可扩展解决方案 C.SQS 无法直接将数据发送到 dynamodb,此处丢失的片段太多D.Lambda 无法支持搜索,而 MySQL 并非最佳选择存储元数据以供搜索

Question 135 **11/19考试原题 03/23考题**

解决方案架构师正在重新设计图像查看和消息传递平台,以作为SaaS.当前,有一个虚拟桌面基础结构(VDI)服务器场运行桌面映像, 查看应用程序和桌面消息传递应用程序.两个应用程序使用共享

数据库来管理用户帐户和共享.用户从启动门户网站的 Web 门户登录应用程序并在用户计算机上流式传输应用程序的视图.发展历程

运营团队希望不再使用 VDI,而是要重写应用程序.

提供安全性和易管理性的 MOST 高性价比架构是什么?

1. 从一个带有单独的 S3 存储桶的 Amazon S3 存储桶运行一个网站,以存储图像和消息传递数据.从嵌入式 JavaScript 调用 AWS Lambda 函数以管理动态内容,并将 Amazon Cognito 用于用户和共享管理.
2. 从 Amazon EC2 Linux 服务器运行一个网站,将图像存储在 Amazon S3 中,并将 Amazon Cognito 用于用户帐户和共享.通过使用 EC2 用户数据来安装和配置应用程序,创建 AWS CloudFormation 模板以启动应用程序.
3. 将网站作为 AWS Elastic Beanstalk 应用程序运行,将图像存储在Amazon S3 中,并将 Amazon RDS

数据库用于用户帐户和共享.创建 AWS CloudFormation 模板以启动应用程序并执行蓝色/绿色部署.

1. 从一个 Amazon S3 存储桶运行一个网站,该网站授权 Amazon AppStream 可以为组合的图像查看器和 Messenger 传输应用程序,以将图像存储在 Amazon S3 中.让网站将 Amazon RDS 数据库用于用户帐户和共享.

答案: C

解释:

在 s3 中传送数据不是一个好主意. Cognito 无法很好地处理共享

Question 136

一家公司希望通过使用 Amazon API Gateway 实施无服务器应用程序, AWS Lambda 和 Amazon DynamoDB.他们部署了概念证明,并指出

平均响应时间大于其上游服务可以接受的亚马逊时间

CloudWatch 指标未表明 DynamoDB 有任何问题,但显示了一些 Lambda

功能正在超时.

解决方案架构师应考虑采取以下哪些行动来提高性能? (选择两个.)

1. 配置 AWS Lambda 函数以重用容器,以避免不必要的启动时间.
2. 增加内存量并调整 Lambda 函数的超时.进行完整的性能测试,以确定 Lambda 函数的理想内存和超时配置.
3. 创建一个运行 Memcached 的 Amazon ElastiCache 集群,并配置 Lambda 函数以进行 VPC 集成并访问 Amazon ElastiCache 集群.
4. 在 Amazon API Gateway 的适当阶段启用 API 缓存,并为需要比整个阶段 TTL 更低的单个方法覆盖

TTL.

1. 增加 CPU 数量,并调整 Lambda 函数的超时.完成性能测试,以确定 Lambda 功能的理想 CPU 和超时配置.

答案: BD

解释:

您不能为 lambda 增加 CPU. CPU 与内存有关

https://docs.aws.amazon.com/lambda/latest/dg/resource-model.html

Question 137 **03/23考题**

一家公司正在将应用程序迁移到 AWS.它希望尽可能多地使用完全托管的服务在迁移期间尽可能.公司需要在其中存储大型重要文件

具有以下要求的应用程序:

-数据必须高度持久且可用.

-静止和传输期间,必须始终对数据进行加密.

-加密密钥必须由公司管理并定期地.轮换

解决方案架构师应推荐以下哪些解决方案?

1. 以文件网关模式将存储网关部署到 AWS.使用使用 AWS KMS 密钥的 Amazon EBS 卷加密来加密存储网关卷.
2. 将 Amazon S3 与存储桶策略一起使用,以对存储桶的连接强制实施 HTTPS,并对对象加密实施服务器端加密和 AWS KMS.
3. 使用具有 SSL 的 Amazon DynamoDB 连接到 DynamoDB.使用 AWS KMS 密钥加密静态 DynamoDB

对象.

1. 部署带有附加的 Amazon EBS 卷的实例以存储此数据.使用使用 AWS KMS 密钥的 EBS 卷加密来加密数据.

答案: B

解释:

A.文件网关链接到 S3,也需要加密 S3 D.您可能无法旋转密钥

Question 138 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

解决方案架构师正在为亚马逊集群设计一个高度可用且可靠的解决方案

EC2 实例.

解决方案架构师必须确保集群中的所有 EC2 实例都能恢复系统发生故障后自动发生.解决方案必须确保恢复的实例 保持相同的 IP 地址.

如何满足这些要求?

A.创建一个 AWS Lambda 脚本以重新启动任何意外关闭的 EC2 实例. B.为最小和最大大小为 1 的每个 EC2 实例创建一个 Auto Scaling 组.

1. 创建一个新的 t2.micro 实例以监视群集实例.配置 t2.micro 实例,使其在失败时发出 aws ec2 reboot- instances 命令.
2. 为 StatusCheckFailed\_System 指标创建一个 Amazon CloudWatch 警报,然后配置 EC2 操作以恢复实例.

答案: D

解释:

B.私有 IP 可能会更改 D.StatusCheckFailed\_System 是针对系统问题的,这就是问题要求的https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status- check.html＃types-of-instance-status-checks

Question 139 **11/19考试原题 类似 03/23考题**

公共零售 Web 应用程序在 Amazon EC2 之前使用应用程序负载平衡器(ALB) 在由 Amazon 支持的区域中跨多个可用区(AZ)运行的实例

RDS MySQL 多可用区部署.目标组运行状况检查配置为使用 HTTP 和指向产品目录页面. Auto Scaling 配置为维持 Web 机群大小

根据 ALB 健康检查.

最近,该应用程序发生了故障. Auto Scaling 不断取代了中断期间的实例.随后的调查确定 Web 服务器指标

处于正常范围内,但是数据库层正在承受高负载,从而导致 严重提高了查询响应时间.

进行以下哪些更改可在改善效果的同时纠正这些问题

监视整个应用程序堆栈的可用性和功能的功能,以备将来使用 增长? (选择两个.)

1. 为 Amazon RDS MySQL 配置只读副本,并在 Web 应用程序中使用单个读取器终端节点以减少后端数据库层的负载.
2. 配置目标组运行状况检查以指向简单的 HTML 页面而不是产品目录页面,并针对该产品页面进行Amazon Route 53 运行状况检查以评估完整的应用程序功能.配置 Amazon CloudWatch 警报以在站点发生故障时通知管理员.
3. 配置目标组运行状况检查,以对产品页面使用 Amazon EC2 Web 服务器的 TCP 检查和 Amazon Route 53 运行状况检查,以评估完整的应用程序功能.配置 Amazon CloudWatch 警报以在站点发生故障时通知管理员.
4. 为 Amazon RDS 配置 Amazon CloudWatch 警报,并采取措施恢复数据库层中高负载,受损的 RDS 实例.
5. 配置一个 Amazon ElastiCache 集群,并将其放置在Web 应用程序和 RDS MySQL 实例之间,以减少后端数据库层的负载.

答案: BE

解释:

B.在 Route 53 级别上的完整堆栈运行状况检查可以减少大量请求,因为我们不需要检查每个实例 C. ALB 的 目 标 组 运 行 状 况 检 查 需 要 为 HTTP 或 HTTPS. 对 于 TCP, 您 将 需 要 NLB https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health -checks.html

Question 140 **12/12考试原题**  **03/09考试原题 03/23考题**

一家公司正在多个 AWS 区域中运行电子邮件应用程序.公司使用俄亥俄州(us-east-1)为主要灾区,北弗吉尼亚(us-east-1)为主要灾区 恢复(DR)区域.数据从主区域连续复制到灾难恢复

在两个区域的公共子网上按单个实例进行区域划分.复制消息 在一天中的某些时段,各地区之间的订单积压很大.积压

会在短时间内自行清除,但会影响应用程序的 RPO.

以下哪个解决方案应有助于修复此性能问题? (选择两个) A.增加实例的大小.

1. 让主要区域中的实例将数据写入主要区域中的 Amazon SQS 队列,并让 DR Region 中的实例从该队列中轮询.
2. 在主区域和灾难恢复区域上使用多个实例来发送和接收复制数据.
3. 将 DR Region 更改为 Oregon(us-west-2),而不是当前的 DR Region.
4. 将一个附加的弹性网络接口附加到两个区域中的每个实例,并在网络接口之间建立负载平衡.

答案: BC

解释:

B.这可能是一个很好的解决方案,因为它可以双向扩展

Question 141 **12/12考试原题** **11/19考试原题**  **03/09考试原题**

一家公司已实施 AWS 组织.它最近建立了一些新的

帐户,并希望拒绝访问这些新帐户中的一组特定的 AWS 服务. 如何有效控制 MOST?

A.在每个拒绝访问服务的帐户中创建一个 IAM 策略.将策略与 IAM 组关联,并将所有 IAM 用户添加到该组. B.创建一个拒绝访问服务的服务控制策略.将所有新帐户添加到单个组织单位(OU),并将策略应用于该OU.

1. 在每个拒绝访问服务的帐户中创建一个 IAM 策略.将策略与 IAM 角色相关联,并指示用户使用其公司凭据登录并承担 IAM 角色.
2. 创建一个拒绝服务访问的服务控制策略,并将该策略应用于组织的根.

答案: B

Question 142 **12/12考试原题**  **03/09考试原题**

一家公司计划将应用程序从本地迁移到 AWS.应用程序

当前使用的是 Oracle 数据库,该公司可以忍受 1 小时的短暂停机

执行向新基础架构的切换.作为迁移的一部分,数据库引擎将

改为 MySQL.解决方案架构师需要确定可以使用哪些 AWS 服务用于执行迁移,同时最大程度地减少所需的工作量和时间.

以下哪项符合要求?

1. 使用 AWS SCT 生成架构脚本,然后在迁移之前将其应用于目标.使用 AWS DMS 分析当前模式,并为最佳数据库引擎提供建议.然后,使用 AWS DMS 迁移到推荐的引擎.使用 AWS SCT 来确定可以转换应用程序中的哪些嵌入式 SQL 代码以及必须手动完成的操作.
2. 使用 AWS SCT 生成架构脚本,然后在迁移之前将其应用于目标.使用 AWS DMS 开始将数据从本地数据库移至 AWS.初始副本之后,继续使用 AWS DMS 保持数据库异步,直到切换到新数据库为止.使用AWS SCT 来确定可以转换应用程序中的哪些嵌入式 SQL 代码以及必须手动完成的操作.
3. 在直接在 Amazon EC2 上安装数据库引擎或迁移到Amazon RDS 之间,使用 AWS DMS 帮助确定最佳的目标部署.然后,使用 AWS DMS 迁移到平台.使用 AWS Application Discovery Service 来确定可以转换应用程序中的哪些嵌入式 SQL 代码以及必须手动执行的操作.
4. 使用 AWS DMS 开始将数据从本地数据库移动到 AWS.初始副本之后,继续使用 AWS DMS 保持数据库同步,直到切换到新数据库为止.使用 AWS Application Discovery Service 来确定可以转换应用程序中的哪些嵌入式 SQL 代码以及必须手动执行的操作.

答案: B

解释:

A. 默 认 情 况 下 , 引 擎 将 始 终 为 innodb https://docs.aws.amazon.com/dms/latest/userguide/CHAP\_Target.MySQL.html B.https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/CHAP\_Converting.App.html https: //aws.amazon.com/dms/faqs/ C.Application Discovery 服务仅不用于此..

Question 143

解决方案架构师已为三层应用程序创建了一个 AWS CloudFormation 模板包含运行自定义 AMI 的 Amazon EC2 实例的 Auto Scaling 组.

解决方案架构师希望确保将来可以部署自定义 AMI 的更新首先更新模板以引用新的 AMI,然后调用它来运行堆栈UpdateStack 将 EC2 实例替换为从新 AMI 启动的实例.

如何部署 AMI 更新以满足这些要求?

1. 为模板的新版本创建一个更改集,查看对运行中的 EC2 实例的更改以确保 AMI 被正确更新,然后执行更改集.
2. 在模板中编辑 AWS :: AutoScaling :: LaunchConfiguration 资源,将其更改为 Replace.删除政策
3. 在模板中编辑 AWS :: AutoScaling::AutoScalingGroup 资源,插入属性.UpdatePolicy
4. 从更新的模板创建一个新的堆栈.成功部署后,修改 DNS 记录以指向新堆栈,然后删除旧堆栈. 答案: C

Question 144

贵公司有一个日志记录微服务,用于在用户有以下情况时生成日志: 在另一个应用程序中输入了某些命令.此日志记录服务是通过

EC2 实例正在侦听的 SQS 标准队列.但是,您发现

在某些情况下,不维护日志的顺序.结果,使用它变得更加困难 跟踪用户活动的服务.您应该如何以简单的方式解决此问题?

A.将现有的标准队列转换为 FIFO 队列.为发送到队列的消息添加重复数据删除 ID. B.删除现有的标准队列,并将其重新创建为 FIFO 队列.结果,确保了接收消息的顺序. C.将整个微服务应用程序迁移到 SWF,以确保操作顺序.

D.错误的时间戳顺序是 SQS 的局限性,尚无解决方法.

答案: B

解释:

A.不能这样做https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO- queues.html#FIFO-queues-moving

Question 145

一家大型贸易公司正在使用内部部署系统来分析贸易数据.交易日关闭后,包括当天交易成本,执行报告和 市场表现在内的数据将发送到 Redhat 服务器,该服务器运行大数据分析工具以预测第二天的交易.

bash 脚本用于配置资源并计划何时运行数据分析工作负载. 应如何使用适当的工具将本地系统迁移到 AWS? (选择三个)

A.创建一个 S3 存储桶以存储用于后处理的交易数据. B.将交易数据从各种来源发送到专用的 SQS 队列.

1. 使用 AWS Batch 通过适当的作业定义执行 bash 脚本.
2. 创建具有自动扩展功能的 EC2 实例,以处理大数据分析工作负载.
3. 使用 CloudWatch Events 安排数据分析作业答案: ACD

Question 146

一家大型 IT 公司拥有一个本地网站,该网站向用户提供房地产信息,例如租金,房价和最新消息.该网站具有 Java 后端和用于存储订户数据的 NoSQL MongoDB 数据库.您是云分析师,需要将整个应用程序迁移到 AWS 平台.您的经理要求在 AWS 中部署类似的结构以实现高可用性.

此外,跟踪框架是必不可少的,它可以记录来自客户端请求和对 AWS 中数据库的下游调用的数据. 您应该选择哪种 AWS 服务来实施迁移?选择 3 选项.

1. 部署 Java 后端服务器的自动伸缩组以提供高可用性
2. 使用 RDS Aurora 作为订户数据的数据库,因为它具有很高的可用性,并且可以扩展到 15 个只读副本
3. 创建一个 DynamoDB 数据库来保存订户数据.为读/写吞吐量设置自动缩放策略.
4. 使用 AWS X-Ray SDK 记录有关传入和传出请求的数据.在 X-Ray 控制台中查看统计信息图.
5. 使用 AWS JAVA SDK 跟踪请求,并将日志发送到 AWS CloudWatch Events.创建一个 CloudWatch 仪表板以查看统计信息.

答案: ACD

Question 147

您在一家视频游戏公司工作,而您的团队正在研究一项功能,该功能可以告诉您查看或单击某些网页的次数.您还创建了一个 AWS Lambda 函数,以显示数据的一些关键统计信息.您测试了 Lambda 函数,它运行完美.

但是,您的团队负责人要求您每天在格林尼治标准时间上午 8:00 在大电视屏幕上显示统计信息,以便当员工每天早上进办公室时,他们对功能的运行方式有一个大概的了解.

实现这一目标的最经济有效的方法是什么?

1. 创建一个使用 cron 表达式调度为 00:08 的 AWS CloudWatch Events 规则,将目标配置为Lambda 函数.
2. 创建一个 Amazon Linux EC2 T2 实例,并使用Crontab 设置一个 Cron 作业.每隔 8:00 AM 使用 AWS CLI 调用您的 AWS Lambda.
3. 使用 Amazon Batch 设置作业,该作业定义为 Lambda 函数每 8:00 AM 运行一次.
4. 在 AWS CloudWatch Events 控制台中,使用 cron 表达式 08:00 单击-reate Event 将目标配置为

Lambda 函数.

答 案 : A Question 148

一家连锁超市在 AWS 中部署了大数据分析系统.系统在 S3 中具有原始数据,例如点击流或过程日志.一个m3.large EC2 实例将数据转换为其他格式,并将其保存到另一个 S3 存储桶中.之后,Amazon Redshift 分析了数据.

您的团队负责使用 AWS Glue(一种完全托管的 ETL(提取,转换和加载)服务)改进系统.

重建大数据系统期间,AWS Glue 可以简化哪些任务? (选择两个)

A.AWS Glue 包含一个连接到 S3 存储桶并扫描数据集的搜寻器.然后,该服务在数据目录中创建元数据表.

B. AWS Glue 自动用 Java 生成代码以从源中提取数据并转换数据以匹配目标架构. C.默认情况下,AWS Glue 创建一个调度程序以每分钟触发一次激活的任务.

D. AWS Glue 具有中央元数据存储库(数据目录).目录中的数据可立即用于分析. 答案: AD

Question 149

AWS 解决方案架构师注意到,他们的公司几乎完全将 EBS 通用 SSD(gp2)卷类型用于其 EBS 卷.他们正在考虑修改其中一些卷的类型,但是不影响性能非常重要.

解决方案架构师可以考虑采取以下哪些行动? (选择两个)

A.可以将 50GB gp2 根卷修改为 EBS 配置的 IOPS SSD(io1),而无需停止实例. B.作为根卷需要附加到实例的 gp2 卷可以修改为吞吐量优化 HDD(st1)卷.

1. 作为非根卷附加到实例的 1GB gp2 卷可以修改为 Cold HDD(sc1)卷.
2. 作为非根卷附加到实例的 1TB gp2 卷可以修改为吞吐量优化 HDD(st1)卷,而无需停止实例或分离卷.

答案: AD

解释:

B.这不可能发生

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/modify-volume-requirements.html C.由于 SC1 的最小大小为 500GB,因此无法使用

https://aws.amazon.com/ebs/features/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/modify-volume-requirements.html

Question 150

以下哪项与使用" HLS"方法观看 Kinesis 视频相关联流? (选择两个)

1. 一个 Web 应用程序,它能够使用第三方播放器 Video.js 显示视频流.
2. 为了处理 Kinesis 视频流,SAAS 提供者需要构建一个新的视频播放器已集成到其主要的在线产品中.
3. 只能观看直播视频,不能观看存档视频.
4. 通过在 Apple Safari 浏览器的位置栏中键入 HLS 流会话 URL 来播放视频,以进行调试.

答案: AD

解释:

B.您不需要播放器来处理视频流 C.可以处理实时视频和点播视频https://aws.amazon.com/blogs/aws/amazon-kinesis-video-streams-adds-support- for-hls-output- streams /D.可以与浏览器一起使用 https://docs.aws.amazon.com/kinesisvideostreams/latest/dg/ API\_reader\_GetHLSStreamingSessionURL.html

Question 151

一个团队刚刚收到一项任务,该任务是构建一个需要识别流视频中的面部的应用程序.他们将从第三方使 用容器格式(MKV)获取源视频.

APP 应该能够通过视频快速实时处理人脸,并以适当的方式保存输出以供下游处理.根据 AWS 解决方案架构师同事的建议,他们希望使用AWS Rekognition 开发服务.

需要以下哪些选项来完成任务?选择 3.

1. S3 存储桶以存储源 MKV 视频,以供 AWS Rekognition 处理. S3 应该是在这种情况下使用,因为它提供了无限的,高度可用的和持久的存储空间. 确保第三方具有对 S3 存储桶的写访问权.
2. Kinesis 视频流,用于将流视频发送到Amazon Rekognition Video.这个可以使用 Java SDK 中的 Kinesis 扬 utMedia API 即可完成. PutMedia 操作写入视频数据片段分成 Amazon Rekognition Video 使用的 Kinesis 视频流.
3. Amazon Rekognition Video 流处理器,用于管理流分析视频.它可以根据需要用于启动,停止和管理流处理器.
4. 使用 EC2 或 Lambda 调用 Rekognition API 揇 etectFaces,并将源视频保存在S3 斗.对于检测到的每个脸部,该操作都会返回脸部详细信息.这些细节包括

人脸的边界框,置信度值和一组固定的属性(例如人脸) 地标等

1. 在 APP 使用 Rekognition API 从实时视频中获取已识别的面部之后,使用

S3 或 RDS 数据库以存储 Rekognition 的输出.另一个 lambda 可以用来对结果进行后处理并呈现给 UI.

1. Kinesis 数据流使用者读取 Amazon Rekognition Video 的分析结果

发送到 Kinesis 数据流.通过添加到以下内容之一,它可以是 Amazon EC2 实例

Amazon 机器映像(AMI).消费者可以通过在多个环境中运行来自动缩放

Auto Scaling 组下的 Amazon EC2 实例.

答案: BCF

解释:

https://docs.aws.amazon.com/rekognition/latest/dg/streaming-video.html

Question 152

一家大公司开始使用具有合并计费功能的 AWS 组织来管理其单独的部门. AWS 运营团队刚刚创建了 3 个 OU(组织单位),每个拥有 2 个 AWS 账户.为了符合公司范围的安全策略,所有已设置的 AWS 账户都需要 CloudTrail.但是,一段时间后,某些 OU 中的用户会关闭其帐户的 CloudTrail.

AWS 运营团队防止这种情况再次发生的最佳方法是什么?

1. 将 AWS Organizations 功能集更新为功能?然后创建服务控制策略(SCP),以防止用户禁用 AWS CloudTrail.这可以是通过使用 cloudtrail:StopLogging 拒绝策略来实现.
2. 这可以通过功能集中的服务控制策略(SCP)来实现.团队需求

删除并重新创建启用了功能的 AWS Organizations,然后使用适当的控制策略来限制cloudtrail:StopLogging 的操作.

1. 在该组织中的每个 AWS 账户中,创建一个 IAM 策略以拒绝包括管理员在内的所有用户的

cloudtrail:StopLogging.

1. 使用服务控制策略(SCP)防止用户禁用AWS CloudTrail.这可以通过允许策略拒绝cloudtrail:StopLogging 来完成

答案: A

解释:

无 需 重 新 创 建 组 织 即 可 启 用 所 有 功 能 集 . https://docs.aws.amazon.com/organizations/latest/userguide/orgs\_manage\_org\_support-all- features.html

Question 153

一家移动应用程序开发人员刚刚在 IOS 和 Android 中制作了一款具有计算步数的功能的应用程序.他使用 AWS Cognito 向用户授权一个用户池和身份池,以提供对 AWS DynamoDB 表的访问.该应用程序使用DynamoDB 表存储用户订户数据和步骤数.

现在,开发人员还需要 Cognito 与 Google 集成,以便为移动应用程序用户提供联合身份验证,以便用户无需记住额外的登录访问权限.

开发人员应该怎么做才能使 IOS 和 Android App 做到这一点?

1. Amazon Cognito 身份池(联合身份)通过以下方式支持用户身份验证联合身份提供者-包括 Amazon,Facebook,Google 和 SAML 身份

提供者.开发人员只需设置联盟身份即可访问 Google

1. 如果 AWS Cognito 需要 Google 访问权限,则只有 Android 适用于联合身份. 这可以通过使用 Google 客户 ID 配置 Cognito 身份池来完成.
2. Amazon Cognito 用户池通过联合身份提供商支持用户身份验证-

包括 Amazon,Facebook,Google 和 SAML 身份提供商.开发人员只需要在 Cognito 用户池中为 Google 访问设置联盟身份.

1. 如果需要 Google 访问,则只有 IOS(Objective-C 和 Swift)可用于联合身份适用于 AWS Cognito.这可以通过使用 Google 配置 Cognito 身份池来完成客户编号. Google 联合访问不适用于 android 应用.

答案: A

解释:

用户池无法授权对 AWS 资源的访问.您将需要一个身份池.用户池只是一个用户目录. https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-identity.html

Question 154

一家大公司提供的服务可以处理巨大的点击流数据集,这些数据集通常是由于零售网站上的假日购物流量 或媒体或社交网站的数据网络上的急剧增长所致.

针对其内部部署基础结构分析这些点击流数据集变得越来越昂贵. 随着样本数据集的不断增长,提供及时响应的应用程序越来越少. 该服务正在使用具有 Cascading 的 Hadoop 集群.

他们如何以最佳方式将应用程序迁移到 AWS?

1. 将源数据放入 S3 并将处理服务迁移到AWS EMR hadoop 集群

与级联.使 EMR 能够直接从 S3 存储桶读取和查询数据.将输出写入 RDS 数据库

1. 将源数据放到 Kinesis 流中,然后将处理服务迁移到 AWS lambda,以利用其扩展功能.启用 lambda 可以直接从 Kinesis 流中读取和查询数据.将输出写入 RDS 数据库
2. 将源数据放入 S3 存储桶中,并通过自动将处理服务迁移到 AWS EC2

缩放.确保自动缩放配置具有适当的最大和最小实例数.在 Cloudwatch 仪表板中监控性能.将输出写入

DynamoDB 表以供下游处理.

1. 将源数据放入 Kinesis 流中,并将处理服务迁移到具有 Cascading 的 AWS EMR 集群.使 EMR 能够直接从 Kinesis 流中读取和查询数据.将输出写入 Redshift.

答案: D

解释:

对于大型数据集,将运动学与 EMR 结合使用是有意义的.如果我们仅将数据集存储在 S3 中,则它与本地解决方案的区别不大.

Question 155

一家人工智能创业公司已经使用了许多 EC2 实例.一些实例使用 SQL Server 数据库,而其他实例使用Oracle.由于需要确保数据的安全性,因此需要定期快照.他们希望 SQL Server EBS 卷每 12 小时拍摄一次快照.

但是,对于 Oracle,它每天仅需要快照.

公司应免费选择以下最佳选择?

1. 使用免费的第三方工具(例如 Clive)来管理 EC2 实例生命周期.它可以设计各种

EC2 EBS 卷的备份策略.向 SQL Server EBS 添加 12 小时备份策略卷和对 Oracle EBS 卷的 24 小时备份策略.

1. 在 SQL Server 和 Oracle EBS 卷的名称上添加一个前缀.在 AWS Data Lifecycle Management 控制台中,基于名称前缀创建两个管理策略.例如,将 12 小时备份计划添加到名称以 sql 开头的 EBS 卷中,并将 24 小时备份计划添加到名称以 oracle?开头的 EBS 卷中.
2. 创建一个专用的 Lambda 函数来区分 EC2 EBS 卷并拍摄快照.设置 Cloudwatch Events Rules 来调用

lambda,以便该函数对于 SQL Server 每 12 小时运行一次,对于 Oracle 每 24 小时运行一次.

1. 为 SQL Server 和 Oracle EBS 卷添加不同的标签.在 AWS Data Lifecycle Management 控制台中,基于标签创建两个管理策略.向 SQL Server 生命周期策略添加 12 小时计划,向 Oracle 生命周期策略添加24 小时计划

答案: D

Question 156

软件工程师已选择 API 网关和 Lambda 非代理集成来实现应用程序.

该应用程序是一种数据分析工具,在调用HTTP 端点时会返回一些统计结果.

Lambda 需要与某些后端数据服务(例如 Keen.io)进行通信,但是有可能发生错误,例如请求的数据错误,通信错误等.

lambda 是使用Java 编写的,可能会返回两个异常,分别是 BadRequestException 和

InternalErrorException.

软件工程师应该怎么做才能用正确的 HTTP 返回码在 API 网关中映射这两个异常?

例如,BadRequestException 和 InternalErrorException 分别映射到 HTTP 返回代码 400 和 500.选择 2.

1. 在 API 的集成响应中添加相应的错误代码(400 和 500)

网关

1. 在 API 网关的方法响应上添加相应的错误代码(400 和 500).
2. 将映射逻辑放入 Lambda 本身,以便在发生异常时,会显示错误代码在 JSON 正文中同时返回.
3. 添加集成响应,其中设置了正则表达式模式,例如 BadRequest 或内部错误.将它们与 HTTP 状态代码关联
4. 在设置了正则表达式模式(例如 BadRequest 或

内部错误.将它们与 HTTP 状态代码 400 和 500 关联.

答案: BD

解释:

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-method-settings- method- response.html https://docs.aws.amazon.com/apigateway/latest/developerguide/api -gateway- integration-settings- Integration-response.html

Question 157

一家 IT 公司在AWS 中拥有一个 Web 产品,该产品可为客户提供折扣餐厅信息.

它使用了一个 S3 存储桶(my\_bucket)来存储餐厅数据,例如图片,菜单等. 该产品已部署在 VPC 子网中.

该公司的 Cloud Architect 决定为此 S3 存储桶配置 VPC 端点,以便提高性能.

为了遵守安全规则,要求仅将新的VPC 端点用于与此特定的 S3 存储桶进行通信,另一方面,S3 存储桶仅允许来自该 VPC 端点的读取/写入操作.

Cloud Architect 应该选择哪两个选项来满足安全需求?

1. 对 Amazon S3 使用 VPC 端点策略来限制对 S3 存储桶" my\_bucket"的访问仅允许 VPC 端点对" my\_bucket"执行 S3 操作
2. 修改 EC2 实例的安全组以将出站操作限制到VPC

终结点(如果传出流量目的地是 S3 存储桶" my\_bucket").

1. 在 S3 存储桶" my\_bucket"中,添加一个 S3 存储桶策略,如果源 IP 地址不等于 EC2 公共 IP(使用" NotIpAddress"条件).
2. 对于 S3 存储桶" my\_bucket",请使用 S3 存储桶策略,如果源是,则拒绝所有操作

VPC 端点不等于创建的端点 ID.

1. 在 S3 存储桶" my\_bucket"中创建一个 S3 存储桶策略,该策略拒绝所有操作,除非源 IP 地址等于 EC2

公共 IP(使用" IpAddress"条件).

答案: AD

Question 158

您可以作为 AWS 解决方案架构师为电子商务零售商工作.贵公司希望与其他第三方合作以改善客户忠诚度计划,以提供更多

全面选择客户奖励.您计划使用 Amazon 托管区块链来实施区块链网络,使您的公司和第三方可以共享和验证快速透明地奖励信息.

您如何为该区块链添加成员?

1. 设置了 Amazon Managed Blockchain 后,AWS 账户中就有一个初始成员.然后,可以在无需发送邀请的情况下将新成员添加到此 AWS 账户中,或者可以为其他 AWS 账户中的成员创建网络邀请
2. 配置了 Amazon 托管区块链后,AWS 账户中就有一个初始成员.然后,无需发送邀请即可将新成员添加到此 AWS 账户中.您无法为其他 AWS 账户添加新成员
3. 创建 Amazon 托管区块链时,AWS 账户中没有任何成员.然后,可以通过发出邀请将新成员添加到此

AWS 账户或其他账户中.

1. 首次创建 Amazon Managed Blockchain 时,AWS 账户中没有任何成员.然后可以在此 AWS 账户中添加新成员.对于其他账户,他们可以使用网络 ID 加入该净区块链网络.

答案: A

解释:

https://docs.aws.amazon.com/managed-blockchain/latest/managementguide/get-started-create- network.html

Question 159 **12/12考试原题** **11/19考试原题**  **03/09考试原题**

一家公司已将应用程序部署到 AWS 的多个环境中,包括生产和测试.**该公司拥有用于生产和测试的单独帐户,并且允许用户根据需要为团队成员或服务创建其他应用程序用户**.安全团队已要求运营团队通过**对安全凭证的集中控制**以及改善环境之间的权限管理,在生产和测试之间实现更好的隔离.

MOST 可以安全地完成以下哪个选项?

1. 创建一个新的 AWS 账户来保存用户和服务账户,例如身份账户.在身份帐户中创建用户和组.在生产和测试帐户中创建具有适当权限的角色.将身份帐户添加到角色的信任策略中.
2. 修改生产和测试帐户中的权限,**以将新的 IAM 用户的创建限制为运营团队的成员**.在每个帐户上设置严格的 IAM 密码策略.在每个帐户中创建新的 IAM 用户和组,以限制开发人员仅访问完成其职务所需的服务. C.创建一个在每个帐户上运行的脚本,该脚本检查用户帐户是否遵守安全策略.禁用任何不符合要求的用户或服务帐户.

D.在生产帐户中创建所有用户帐户.在生产帐户和测试帐户中创建访问角色.授予从生产帐户到测试帐户 的跨帐户访问权限.

答案: B

Question 160 **11/19考试原题**

一家拥有多个 IT 部门且每个部门都有自己的 AWS 帐户的大型企业的 CIO 希望在一个中央位置管理用户的 AWS 权限,并可以将用户身份验证凭证与公司现有的本地解决方案同步.

哪种解决方案可以满足 CISO 的要求?

1. 根据中央账户中用户的功能职责定义 AWS IAM 角色.创建一个基于 SAML 的身份管理提供程序.将本地组中的用户映射到 IAM 角色.在其他帐户和中央帐户之间建立信任关系.
2. 使用 AWS Organizations 在所有AWS 账户中部署一组通用的 AWS IAM 用户,组,角色和策略.在本地身份提供程序和 AWS 账户之间实施联合.
3. 在集中式帐户中使用 AWS Organizations 定义**服务控制策略(SCP)**.在每个帐户中创建一个基于 SAML

的身份管理提供程序,并将本地组中的用户映射到 AWS IAM 角色.

1. 对用户群进行彻底分析,并创建具有必要权限的 AWS IAM 用户账户.设置一个过程以根据本地解决方案中的数据进行预配和预配.

答案: C

Question 161 **12/12考试原题**  **03/09考试原题**

随着时间的推移,一家大公司以一种不受管理的方式提高了对 AWS 的利用率.因此,他们在不同业务部门, 项目和环境中拥有大量独立的 AWS 账户.该公司已经创建了一个云卓越中心团队,该团队负责管理 AWS 云的各个方面,包括其 AWS 账户.

卓越云中心团队应采取以下哪些措施以最好地解决他们的问题:

集中要求? (选择 2个.)

1. **控制所有 AWS 账户根用户凭证**.在需要访问 AWS 资源的每个用户的账户中分配 AWS IAM 用户.在向每个用户分配权限时,遵循最小特权策略.
2. 用有关业务部门,项目和环境的详细信息标记所有 AWS 资源.将所有 AWS 成本和使用情况报告发送到中央 Amazon S3 存储桶,并使用Amazon Athena 和 Amazon QuickSight 之类的工具按业务部门收集账单明细.
3. 使用 AWS Marketplace 选择和部署成本管理工具.用有关业务部门,项目和环境的详细信息标记所有

AWS 资源.将 AWS 账户的所有 AWS 成本和使用情况报告发送到此工具进行分析.

1. 设置 AWS 组织.**启用整合账单**,并将所有现有AWS 账户链接到主账单账户.用有关业务部门,项目和环境的详细信息标记所有 AWS 资源.使用 Amazon Athena 和 Amazon QuickSight 之类的工具分析"成本和使用情况"报告,以按业务部门收集账单明细.
2. 使用一个主 AWS 账户,在该主账户中创建 IAM 用户.在其他 AWS 账户中定义 IAM 角色,这些角色涵盖了该账户中的每个必需功能.在分配权限给每个角色时遵循最小特权策略,然后使IAM 用户承担角色

他们需要使用的. 答案: AD

Question 162 **11/19考试原题**

为了遵守行业法规,解决方案架构师必须设计一种解决方案,将公司的关键数据存储在多个公共AWS 区域中,包括公司总部所在的美国.解决方案架构师需要向公司的全球 WAN 网络提供对存储在 AWS 中的数据的访问权限.安全团队要求所有访问此数据的流量都不得经过公共互联网.

解决方案架构师应如何设计满足要求并具有成本效益的高可用性解决方案?

1. 建立从公司总部到正在使用的所有 AWS 区域的 AWS Direct Connect 连接.使用公司 WAN 将流量发送到总部,然后再发送到相应的 DX 连接以访问数据.
2. 建立从公司总部到 AWS 区域的两个 AWS Direct Connect 连接.使用公司的 WAN 通过 DX 连接发送流量.**使用区域间 VPC 对等**访问其他 AWS 区域中的数据.
3. 建立从公司总部到 AWS 区域的两个 AWS Direct Connect 连接.使用公司的 WAN 通过 DX 连接发送流量.使用 AWS 过渡 VPC 解决方案来访问其他 AWS 区域中的数据.
4. 建立从公司总部到 AWS 区域的两个 AWS Direct Connect 连接.使用公司的 WAN 通过 DX 连接发送流量.使用 Direct Connect 网关访问其他 AWS 区域中的数据.

答案: B

Question 163 **12/12考试原题**  **03/09考试原题**

一家公司希望通过迁移到 AWS 来管理与一组 20 个**关键应用程序**相关的成本.这些应用程序是 Java 和Node.js 的混合,分布在不同的实例群集中.该公司希望在使用**单一部署方法进行标准化的同时将成本降至最低**.大多数应用程序是具有少量并发用户的月末处理例程的一部分,但有时会在其他时间运行.平均

尽管某些应用程序在高峰处理期间使用多达 2.5 GB 的内存,但应用程序的内存消耗少于 1 GB.该组中最重要的应用程序是用 Java 编写的计费报告,该报告可访问多个数据源,并且**通常需要几个小时**.

哪种是最具成本效益的解决方案?

1. 为每个应用程序部署一个单独的 *AWS Lambda 函数*.使用 AWS CloudTrail 日志和 Amazon CloudWatch 警报来验证关键作业的完成.
2. 在配置了 Auto Scaling 的 *Amazon EC2 上部署 Amazon ECS 容器*,以实现 75%的内存利用率.通过ECS 任务扩展,为要迁移的每个应用程序部署 ECS 任务.使用 Amazon CloudWatch 监控服务和主机.
3. 使用自动扩展功能为每个应用程序部署 AWS Elastic Beanstalk,以确保所有请求都具有足够的资源.使用 CloudWatch 警报监视每个 AWS Elastic Beanstalk 部署.
4. 部署一个新的 *Amazon EC2 实例集群*,该集群通过使用 EC2 Auto Scaling 和应用程序负载平衡器共同托管所有应用程序.基于实例内存利用率的自定义指标集来扩展集群大小.*购买 3 年的预留实例预留*,该预留等于 Auto Scaling 组的 GroupMaxSize 参数.

答案: C

**解释（张）：**

[**https://docs.aws.amazon.com/zh\_cn/lambda/latest/dg/best-practices.html**](https://docs.aws.amazon.com/zh_cn/lambda/latest/dg/best-practices.html)

**使用 AWS Lambda 函数的最佳实践**

[**https://docs.aws.amazon.com/zh\_cn/lambda/latest/dg/gettingstarted-limits.html**](https://docs.aws.amazon.com/zh_cn/lambda/latest/dg/gettingstarted-limits.html)

**AWS Lambda 配额**

Lambda有一定限制，默认并发上限为1000次

函数内存分配：128 MB 到 3,008 MB，以 64 MB 为增量。

函数超时：900 秒（15 分钟）

对您的 Lambda 函数进行性能测试是确保选择最佳内存大小配置的关键环节。增加内存大小会触发函数可用 CPU 的同等水平的增加。

**托管服务优先**：如果有合适的托管服务（Beanstalk、RDS、SQS、NAT网关等），EC2不是优先选择，EC2上搭建自己DB实例基本上不是好的实践。

**长效机制优先：“经常更新”“更频繁的执行”等做法不是好的做法；设置触发机制（Cloud Watch Event规则+Lambda函数）、设置预设方案（AWS Catalog产品组合）是更好的做法。**

**※懒人原则：有简单的做法，就不要自己一个一个自己来设置**

**最小权限原则：**仅给予其需要的最小原则。最好是设置代理（角色、组、动态临时凭证STS），而不是直接分配权限和凭证给实体账户。

Question 164 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

解决方案架构师必须为在手机平台上运行的流行的全球视频游戏构建高度可用的基础架构.该应用程序在Application Load Balancer 后面的 Amazon EC2 实例上运行.实例在多个可用区中的 Auto Scaling 组中运行.数据库层是 Amazon RDS MySQL.多可用区实例.整个应用程序堆栈都部署在 us-east-1 和 eu- central-1 中. Amazon Route 53 用于使用基于延迟的路由策略将流量路由到两个安装.如果在区域 53 中的安装无响应,则在Route 53 中将加权路由策略配置为故障转移到另一个区域.

在灾难恢复场景的测试期间,在阻止从该区域中运行的所有应用程序实例访问 eu-central-1 中的 Amazon RDS MySQL 实例之后.Route 53 不会自动将所有流量故障转移到 us-east-1.根据这种情况,

哪些更改将允许基础结构故障转移到 us-east-1?(选择两个.)

1. 在 us-east-1 中,指向记录的权重为 100；在 eu-central-1 中,指向记录的权重为 60.
2. 在 us-east-1 中为指向主应用程序负载均衡器的记录指定权重 100,在 eu-central-1 中为指向主应用程序负载均衡器的记录指定权重 0.
3. 在 eu-central-1 和 us-east-1 的延迟别名资源上,将"评估目标健康状况"的值设置为"是".
4. 在*应用程序中编写一个 URL,以*在数据库层上执行运行状况检查.将其作为健康检查添加到两个区域的加权路由策略中.

答案: BC

Question 165 **11/19考试原题 03/23考题**

在线电子商务业务正在 AWS 上运行工作负载.该应用程序体系结构包括一个 Web 层,一个用于业务逻辑的应用程序层以及一个用于用户和事务数据管理的数据库层.数据库服务器的内存需求为 100 GB.业务需要以 5 分钟的 RTO 和 1 小时的 RPO 对应用程序进行具有成本效益的灾难恢复.该公司还具有针对区域外灾难恢复的法规,主要站点和备用站点之间的最小距离为 250 英里.

Solutions Architect 可以设计以下哪个选项来为该客户创建满足灾难恢复要求的全面解决方案?

1. *经常备份*应用程序和数据库数据,然后将它们复制到 Amazon S3.使用 S3 跨区域复制来复制备份,并使用 AWS CloudFormation 实例化基础架构以进行灾难恢复并从 Amazon S3 恢复数据.
2. 使用一个先导环境,在该环境中,主数据库配置有镜像,以在备用区域中的 m4.large 上构建备用数据库. 在发生灾难时,使用 AWS CloudFormation 实例化Web 服务器,应用程序服务器和负载均衡器,以在备用区域中启动应用程序.垂直调整数据库的大小以满足全部生产需求,然后使用 Amazon Route 53 将流量切换到备用区域.
3. 在备用区域中使用功能完整的生产环境的缩减版本,该备用环境包括 Web 服务器的一个实例,应用程序服务器的一个实例以及处于待机模式的数据库服务器的复制实例.将 Web 和应用程序层放置在负载均衡

器后面的 Auto Scaling 中,该负载均衡器可以在负载到达应用程序时自动缩放.使用 Amazon Route 53 将流量切换到备用区域.

1. 使用具有两个功能完全相同的 Web,应用程序和数据库层的多区域解决方案.仅在一个区域中激活主数据库,而在另一区域中激活备用数据库.使用 Amazon Route 53 通过运行状况检查路由策略自动将流量从一个区域切换到另一区域

答案: D

Question 166 **12/12考试原题** **11/19考试原题**  **03/09考试原题**

一家公司使用按需 Amazon EC2 计算优化实例运行内存密集型分析应用程序.该应用程序被连续使用,并且在工作时间内应用程序需求翻倍.该应用程序当前根据 CPU 使用量进行扩展.发生扩展时,将使用生命周期挂钩,因为实例需要 4 分钟才能在终止之前清除应用程序状态.

由于用户报告在工作时间内性能不佳,因此实施了计划的扩展操作,因此将在工作时间内添加其他实例.已 要求解决方案架构师降低应用程序成本.

哪种解决方案最符合成本效益?

1. 使用使用 C5 实例的现有启动配置,并更新应用程序 AMI 以包括Amazon CloudWatch 代理.更改自动扩展策略以根据内存利用率进行扩展.将预留实例用于下班后所需的实例数,并使用竞价型实例来满足工 作时间内不断增长的需求.
2. 更新现有的启动配置以使用 R5 实例,并更新应用程序 AMI 以包括 SSM 代理.更改自动扩展策略以根据内存利用率进行扩展.将预留实例用于下班后所需的实例数,并使用竞价型实例和按需实例来满足工作时间内不断增长的需求.
3. 使用使用 C5 实例的现有启动配置,并更新应用程序 AMI 以包括 SSM 代理.保留"自动缩放"策略以根据

CPU 利用率进行缩放.将计划的预留实例用于下班后所需的实例数,并使用竞价型实例以满足工作时间的需求增长.

1. 使用 R5 实例创建新的启动配置,并更新应用程序 AMI 以包括 Amazon CloudWatch 代理.更改自动扩展策略以根据内存利用率进行扩展.将预留实例用于下班后所需的实例数,并使用标准预留实例和按需实 例来满足工作时间内不断增长的需求.

答案: A

Question 167 **11/19考试原题**

一家公司希望使用面向全球客户的无服务器架构设计模式在 AWS 上关注其网站.该公司概述了其要求如下:

-网站应具有响应能力.

-网站应提供最小的延迟.

-该网站应具有很高的可用性.

-用户应该能够通过社交身份提供商(例如 Google,Facebook 和 Amazon)进行身份验证.

-应该有基线 DDoS 保护,以防止流量高峰. 如何满足设计要求?

1. 将 Amazon CloudFront 与 Amazon ECS 结合使用来托管网站.使用 AWS Secrets Manager 提供用户管理和身份验证功能.使用 ECS Docker 容器构建 API.
2. 将 Amazon Route 53 延迟路由与位于不同区域的 Application Load Balancer 和 AWS Fargate 一起使用来托管网站.使用 Amazon Cognito 提供用户管理和身份验证功能.使用 Amazon EKS 容器.
3. 将 Amazon CloudFront 与 Amazon S3 结合使用以托管静态 Web 资源.使用 Amazon Cognito 提供用户管理身份验证功能.结合使用 Amazon API Gateway 和 AWS Lambda 来构建 API.
4. 使用 AWS Direct Connect 与 Amazon CloudFront 和 Amazon S3 托管静态 Web 资源.使用 Amazon Cognito 提供用户管理身份验证功能.使用 AWS Lambda 构建 API.

答案: C

Question 168  **03/09考试原题**

一家公司当前正在使用 AWS CodeCommit 进行源代码控制,并使用 AWS CodePipeline 进行持续集成. 管道具有用于构建工件的构建阶段,然后将该阶段放入 Amazon S3 存储桶中.

公司已经确定了现有流程中的各种改进机会,并且对解决方案架构师提出了以下要求:

-创建新的管道以支持功能开发

-在不影响生产应用程序的情况下支持功能开发

-将连续测试与单元测试相结合

-隔离开发和生产工件

-支持将经过测试的代码合并为生产代码的功能.

解决方案架构师应如何满足这些要求?

1. 从 CodeCommit 功能分支触发一个单独的管道.使用 AWS CodeBuild 运行单元测试.使用 CodeBuild

将工件放在一个单独的测试帐户中的 S3 存储桶中.

1. 从 CodeCommit 功能分支触发一个单独的管道.使用 AWS Lambda 来运行单元测试.使用 AWS CodeDeploy 将工件放在一个单独的测试帐户中的 S3 存储桶中.
2. 从 CodeCommit 标记触发一个单独的管道使用 Jenkins 运行单元测试.在管道中创建一个阶段,以 S3

为目标,以便在单独的测试帐户中使用 S3 存储桶来暂存工件.

1. 创建一个单独的 CodeCommit 存储库以进行功能开发,并使用它来触发管道.使用 AWS Lambda 来运行单元测试.使用 AWS CodeBuild 在同一生产账户中的不同 S3 存储桶中暂存工件.

答案: A

Question 169 **12/12考试原题**  **03/09考试原题**

一家公司使用 Amazon SQS 和 AWS Lambda 在 AWS 上运行订购系统,并且每个订单都以 JSON 消息形式接收.最近,该公司进行了一次营销活动,导致订单增加了十倍.随着这种增加,以下不良行为开始了

订购系统:

-处理订单时 Lambda 故障导致队列积压.

-相同的订单已被处理多次.已要求解决方案架构师解决订购系统中的现有问题,并添加以下弹性功能:

-保留有问题的订单进行分析.

-如果错误超出阈值,则发送通知.

解决方案架构师应如何满足这些要求?

1. 每次 Lambda 调用都会接收多条消息,将错误处理添加到消息处理代码中,并在处理后删除消息,增加消息的可见性超时,为无法处理的消息创建死信队列,并在 Amazon CloudWatch 上创建警报通知的 Lambda 错误.
2. 每次 Lambda 调用都接收单个消息,放置其他 Lambda 工作者以轮询队列,在处理后删除消息,增加消息的消息计时器,将 Amazon CloudWatch Logs 用于无法处理的消息,在 Lambda 上创建 CloudWatch 警报通知错误.
3. 每次 Lambda 调用都会接收多条消息,在接收消息时使用长时间轮询,使用 Amazon CloudWatch Logs 记录来自消息处理代码的错误,使用 AWS Lambda 创建一个死信队列来捕获失败的调用,在以下位置创建CloudWatch 事件

通知的 Lambda 错误.

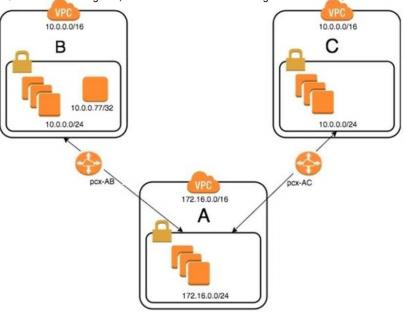
1. 每次 Lambda 调用都会接收多条消息,将错误处理添加到消息处理代码中,并在处理后删除消息,增加消息的可见性超时,为无法处理的消息创建延迟队列,在 Lambda 上创建 Amazon CloudWatch 指标通知错误.

答案: D

Question 170 **11/19考试原题 03/23考题**

一个组织最近通过收购而成长.购买的两家公司使用相同的 IP CIDR 范围.有一个新的短期要求,即允许

AnyCompany A(VPC-A)与 IP 地址为 10.0.0.77 的服务器在 AnyCompany B(VPC-B)中进行通信. AnyCompany A 还必须与 AnyCompany C(VPC-C)中的所有资源进行通信.网络团队已经创建了 VPC 对等链接,但是在 VPC-A 和 VPC-B 之间的通信存在问题.经过调查,团队认为 VPC 中的路由表不正确.



除了 AnyCompany B 中的数据库之外,什么配置将允许 AnyCompany A 与 AnyCompany C 通信? A.在 VPC-A 上,跨 VPC 对等 pcx-AB 为 VPC-B CIDR 范围(10.0.0.0/24)创建一条静态路由.

跨 VPC 对等 pcx-AC 创建 10.0.0.0/16 静态路由.

在 VPC-B 上,为对等 pcx-AB 上的 VPC-A CIDR(172.16.0.0/24)创建一条静态路由.

在 VPC-C 上,跨对等 pcx-AC 为 VPC-A CIDR(172.16.0.0/24)创建静态路由. B.在 VPC-A 上,在 pcx-AB 和 pcx-AC 上启用动态路由传播.

在 VPC-B 上,启用动态路由传播,并使用安全组在 VPC 对等 pcx-AB 上仅允许 IP 地址 10.0.0.77/32.

在 VPC-C 上,使用对等 pcx-AC 上的 VPC-A 启用动态路由传播.

1. 在 VPC-A 上,创建阻止 VPC 对等 pcx-AC 上 IP 地址 10.0.0.77/32 的网络访问控制列表.

在 VPC-A 上,在 pcx-AB 上为 VPC-B CIDR(10.0.0.0/24)创建静态路由,在 pcx-AC 上为 VPC-C CIDR(10.0.0.0/24)创建静态路由.

在 VPC-B 上,跨对等 pcx-AB 为 VPC-A CIDR(172.16.0.0/24)创建静态路由.

在 VPC-C 上,跨对等 pcx-AC 为 VPC-A CIDR(172.16.0.0/24)创建静态路由.

1. 在 VPC-A 上,跨 VPC 对等 pcx-AB 为 VPC-B CIDR(10.0.0.77/32)数据库创建静态路由.

在 VPC 对等 pcx-AC 上为 VPC-C CIDR 创建静态路由.

在 VPC-B 上,为对等 pcx-AB 上的 VPC-A CIDR(172.16.0.0/24)创建一条静态路由.

在 VPC-C 上,跨对等 pcx-AC 为 VPC-A CIDR(172.16.0.0/24)创建静态路由.

答案: D

解释:

VPC-A 仅访问数据库 VPC-B

Question 171 **12/12考试原题** **11/19考试原题**  **03/09考试原题**

一家公司正在 AWS 上设计一个新的高度可用的 Web 应用程序.该应用程序需要从 AWS 中的应用程序服务器到公司的本地环境中托管的后端 REST API 的一致且可靠的连接. AWS 和本地之间的后端连接将通过私有虚拟接口通过 AWS Direct Connect 连接进行路由. Amazon Route 53 将用于管理应用程序的私有 DNS 记录,以解析后端 REST API 上的 IP 地址.

哪种设计可以提供与后端 API 的可靠连接?

1. 为后端 REST API 至少实现两个后端端点,并使用 Route 53 运行状况检查来监视每个后端端点的可用性并执行 DNS 级别的故障转移.
2. 从另一个网络运营商安装第二个 Direct Connect 连接,并将其连接到与第一个 Direct Connect 连接相同的虚拟专用网关.
3. 为来自同一网络运营商的同一直接连接连接安装第二个交叉连接,并将两个连接都连接到同一私有虚拟 接口上的同一链路聚合组(LAG).
4. 创建从本地数据中心到 AWS 的通过公共 Internet 路由的 IPSec VPN 连接,并将其连接到与 Direct Connect 连接相同的虚拟专用网关.

答案: B

Question 172 **03/23考题**

一家零售公司正在运行一个应用程序,该应用程序将发票文件存储在 Amazon S3 存储桶中,并将有关文件的元数据存储在 Amazon 中. S3 存储桶和 DynamoDB 表位于us-east-1 中.该公司希望保护自己免受数据损坏和与任一地区的连接中断的影响.

哪个选项满足这些要求?

1. 创建一个 DynamoDB 全局表以在 us-east-1 和 eu-west-1 之间复制数据.在 us-east-1 中的 DynamoDB

表上启用连续备份.在 S3 存储桶上启用版本控制.

1. 创建一个由 Amazon CloudWatch Events 触发的 AWS Lambda 函数,以对 DynamoDB 表进行常规备份.设置从 us-east-1 到 eu-west-1 的 S3 跨区域复制.在 us-east-1 的 S3 存储桶上设置 MFA 删除.
2. 创建一个 DynamoDB 全局表以在 us-east-1 和 eu-west-1 之间复制数据.在 S3 存储桶上启用版本控制. 在 S3 存储桶上实施严格的 ACL.
3. 创建一个 DynamoDB 全局表以在 us-east-1 和 eu-west-1 之间复制数据.在 us-east-1 中的

DynamoDB 表上启用连续备份.设置从 us-east-1 到 eu-west-1 的 S3 跨区域复制.

答案: D

Question 173 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

一家公司希望在多个国家/地区开设在线购物网站,并且必须确保保护客户免受潜在的"中间人"攻击. 哪种架构将提供 MOST 安全的站点访问权限?

1. 使用 Amazon Route 53 进行域注册和DNS 服务.为所有Route 53 请求启用 DNSSEC.使用 AWS Certificate Manager(ACM)为购物网站注册 TLS / SSL 证书,并为该网站使用配置有那些 TLS / SSL 证书的 Application Load Balancer.在对站点的所有客户端请求中使用"服务器名称标识"扩展.
2. 从第三方证书服务中注册 2048 位加密密钥.使用将DNSSec 的客户托管密钥用于第三方 DNS 提供程序.将密钥上传到 ACM,并使用 NGINX 使用 ACM 自动将安全 Web 服务的证书部署到 EC2 前端 Web 服务器机群.在对站点的所有客户端请求中使用"服务器名称标识"扩展.
3. 使用 Route 53 进行域注册.从第三方证书注册 2048 位加密密钥.对于使用客户托管密钥的 DNS 请求, 请使用支持 DNSSEC 的第三方 DNS 服务.将客户管理的密钥导入 ACM,以将证书部署到配置了站点的TLS / SSL 证书的 Classic Load Balancer.在对站点的所有客户端请求中使用"服务器名称标识"扩展.
4. 使用 Route 53 进行域注册,并在运行 Bind 的 Amazon EC2 实例上托管公司 DNS 根服务器.为 DNS 请求启用 DNSSEC.使用 ACM 为购物网站注册 TLS / SSL 证书,并为该网站使用配置有那些 TLS / SSL 证书的应用程序负载平衡器.在对站点的所有客户端请求中使用"服务器名称标识"扩展.

答案: D

Question 174

公司正在创建一个客户策略,以便他们可以开始使用 AWS.安全团队将为每个团队提供他们遵循原则或最低特权访问所需的权限.团队希望将其资源与其他组隔离开来,财务团队希望将每个团队的资源使用情况分开开票.

哪个帐户创建过程满足这些要求并允许更改?

1. 创建一个新的 AWS Organizations 帐户.在 Active Directory 中创建组,并将其分配给 AWS 中的角色,以授予联合访问权限.要求每个团队标记他们的资源,并根据标记分开帐单.通过 IAM 授予最低要求的特权, 控制对资源的访问.
2. 为每个团队创建个人帐户.将安全性分配为主帐户,并为所有其他帐户启用合并账单.为安全性创建跨帐 户角色以管理帐户,并将日志发送到安全帐户中的存储桶.
3. 创建一个新的 AWS 账户,并使用 AWS Service Catalog 向团队提供所需的资源.实施第三方计费,以根据标签向财务团队提供每个团队的资源使用情况.使用 IAM 隔离资源,以避免帐户泛滥.安全将控制和

监视日志和权限.

1. 使用组织创建一个用于计费的主帐户,并从该主帐户创建每个团队的帐户.创建用于日志和跨帐户访问的安全帐户.在每个帐户上应用服务控制策略,并向安全团队授予对所有帐户的跨帐户访问权限.安全性将 为每个帐户创建 IAM 策略,以维持最少的特权访问.

答案: D

Question 175 **11/19考试原题**  **03/09考试原题 03/23考题**

一家公司在其本地数据中心中拥有 24 TB MySQL 数据库,并且每天以 10 GB 的速度增长.数据中心通过50 Mbps VPN 连接连接到公司的 AWS 基础设施.该公司正在将应用程序和工作负载迁移到AWS.应用程序代码已经

在 Amazon EC2 上安装和测试.该公司现在需要迁移数据库,并希望在 3 周内在 AWS 上发布. 以下哪种方法符合最少停机时间的计划?

A.1.使用 VM Import / Export 服务将本地数据库上的快照导入 AWS.

1. 从快照启动一个新的 EC2 实例.
2. 通过 VPN 设置从本地到 EC2 数据库的持续数据库复制.
3. 更改 DNS 条目以指向 EC2 数据库.
4. 停止复制.
5. 1.启动一个 AWS DMS 实例.
6. 启动一个 Amazon RDS Aurora MySQL 数据库实例.
7. 使用本地和 Amazon RDS 数据库信息配置 AWS DMS 实例.
8. 通过 VPN 在 AWS DMS 中启动复制任务.
9. 更改 DNS 条目以指向 Amazon RDS MySQL 数据库.
10. 停止复制.
11. 1.使用数据库本地工具在本地创建数据库导出. 2.使用 AWS Snowball 将其导入 AWS.
12. 启动一个 Amazon RDS Aurora 数据库实例.
13. 从导出将数据加载到 RDS Aurora 数据库实例中.
14. 设置通过 VPN 从本地数据库到 RDS Aurora 数据库实例的数据库复制.
15. 更改 DNS 条目以指向 RDS Aurora 数据库实例.
16. 停止复制.
17. 1.使本地应用程序脱机.

2.使用数据库本地工具在本地创建数据库导出. 3.使用 AWS Snowball 将其导入 AWS.

1. 启动一个 Amazon RDS Aurora 数据库实例.
2. 从导出将数据加载到 RDS Aurora 数据库实例中.
3. 更改 DNS 条目以指向 Amazon RDS Aurora 数据库实例. 7.放置 Amazon EC2 托管的应用程序

答 案 : C

Question 176 **12/12考试原题** **11/19考试原题**

公司希望允许其营销团队对客户记录执行 SQL 查询,以识别细分市场.数据分布在数百个文件中.记录必须在运输和静止时进行加密.团队管理者必须具有管理用户和组的能力,但是任何团队成员都不能访问 SQL 查询不需要的服务或资源.此外,管理员需要审核所作的查询,并在查询违反安全团队定义的规则时接收通知. AWS Organizations 已用于创建新帐户和具有 Team Manager 管理员权限的 AWS IAM 用户.

哪种设计满足这些要求?

1. 应用服务控制策略(SCP),该策略允许访问 IAM,Amazon RDS 和 AWS CloudTrail.在 Amazon RDS MySQL 中加载客户记录,并培训用户使用 AWS CLI 执行查询.将查询日志从 RDS 数据库实例流式传输到Amazon CloudWatch Logs.将预订过滤器与 AWS lambda 函数配合使用,以针对个人数据的查询进行审计并发出警报.
2. 应用服务控制策略(SCP),该策略拒绝对除 IAM,Amazon Athena,Amazon S3 和 AWS CloudTrail 之外的所有服务的访问.将客户记录文件存储在 Amazon S3 中,并培训用户通过 Athena 使用 CLI 执行查询.分析 CloudTrail 事件以审核并警告查询针对个人数据.
3. 将拒绝所有服务的服务控制策略(SCP)应用到IAM,Amazon DynamoDB 和 AWS CloudTrail 之外.将客户记录存储在 DynamoDB 中,并培训用户使用 AWS CLI 执行查询.启用 DynamoDB 流以跟踪发出的查询, 并使用 AWS Lambda 函数进行实时监视和警报.
4. 应用允许 IAM,Amazon Athena,Amazon S3 和 AWS CloudTrail 使用的服务控制策略(SCP).将客户记录作为文件存储在 Amazon S3 中,并培训用户以利用 Amazon S3 Select 功能并使用 AWS CLI 执行查询. 启用 S3 对象级日志记录并分析 CloudTrail 事件,以针对个人数据的查询进行审核和报警.

答案: B

Question 177 **11/19考试原题**

解决方案架构师负责重新设计旧版 Java 应用程序,以提高其可用性,数据持久性和可伸缩性.当前,该应用程序在单个高内存 Amazon EC2 实例上运行.它接受来自上游客户端的 HTTP 请求,将它们添加到内存队列中,并以 200 状态响应.单独的应用程序线程从队列中读取项目,进行处理,并将结果持久保存到 Amazon RDS MySQL 实例.每个项目的平均处理时间为 90 秒,其中大部分时间用于等待外部服务调用,但是编写该应用程序可并行处理多个项目.此服务的流量不可预测.在高负载期间,项目可能会在应用程序处理备份的过程中在内部队列中放置一个小时以上.此外,如果单个应用程序节点发生故障,当前系统在可用性和数据方面也会存在问题.

访问该服务的客户端不能被修改.他们希望在超时并重试该请求之前的 10 秒钟内收到对发送的每个

HTTP 请求的响应.

哪种方法可以提高系统的可用性和耐用性,同时减少处理延迟并最大程度地降低成本?

1. 创建一个使用 Lambda 代理集成的 Amazon API Gateway REST API,以将请求传递给 AWS Lambda 函数.将核心处理代码迁移到 Lambda 函数,并编写一个包装器类,该包装器类提供一个处理程序方法,该方法将代理事件转换为内部应用程序数据模型并调用处理模块.
2. 创建一个 Amazon API Gateway REST API,该 API 使用服务代理将项目放入 Amazon SQS 队列中.从现有应用程序中提取核心处理代码,并对其进行更新以从 Amazon SQS 队列中提取项目.从现有应用程序中提取核心处理代码,并将其更新以从 Amazon SQS 中提取项目,而不是从内存队列中提取项目.将新的处理应用程序部署到 Auto Scaling 组中较小的 EC2 实例,该组将根据 Amazon SQS 队列中的大约消息数量进行动态扩展.
3. 修改应用程序以使用 Amazon DynamoDB 代替 Amazon RDS.为 DynamoDB 表配置 Auto Scaling.使用基于 CPU 利用率的扩展策略在 Auto Scaling 组中部署应用程序.将带有内存映射文件的内存队列返回实例存储卷,并定期将该文件写入Amazon S3.
4. 更新应用程序以使用 Redis 任务队列而不是内存队列.为应用程序构建一个 Docker 容器映像.创建一个Amazon ECS 任务定义,其中包括应用程序容器和一个用于承载 Redis 的单独容器.使用 AWS Fargate 将新任务定义部署为 ECS 服务,并启用Auto Scaling.

答案: B

Question 178 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

解决方案架构师需要将旧版应用程序从本地迁移到 AWS.在本地,该应用程序在负载均衡器后面的两台Linux 服务器上运行,并访问两台服务器上的 master-master 数据库.每个应用程序服务器都需要一个许可证文件,该文件与服务器的网络适配器的 MAC 地址绑定在一起.通过电子邮件发送新的许可证文件需要软件供应商 12 个小时.该应用程序要求配置文件使用静态.用于访问数据库服务器而不是 DNS 的 IPv4 地址. 鉴于这些要求,

应该一起采取哪些步骤才能为应用程序服务器启用可扩展的体系结构? (选择两个.)

1. 创建一个 ENI 池,向供应商索要该池的许可证文件,并将许可证文件存储在 Amazon S3 中.创建自动化以下载未使用的许可证,并在启动时附加相应的 ENI.
2. 创建一个 ENI 池,向供应商请求该池的许可证文件,将许可证文件存储在 Amazon EC2 实例上,修改配置文件,并从该实例创建 AMI.对所有实例都使用此 AMI.
3. 创建一个引导自动化程序,以使用唯一的退回电子邮件向供应商请求新的许可证文件.让服务器使用接 收到的许可证文件进行自我配置.
4. 创建引导程序自动化以从池中附加 ENI,从 AWS Systems Manager 参数存储中读取数据库 IP 地址,并将这些参数注入本地配置文件.使用 Lambda 函数使 SSM 保持最新.
5. 在 EC2 实例上安装应用程序,配置应用程序,并配置IP 地址信息.从此实例创建一个 AMI,并将 if 用于所有实例.

答案: AD

Question 179 **12/12考试原题** **11/19考试原题**  **03/09考试原题**

公司有一个网站,使用户可以上传视频.公司政策规定,必须对上传的视频进行限制内容分析.已上传的视频 被放置在 Amazon S3 中,并且消息连同视频的位置一起被推送到 Amazon SQS 队列中.后端应用程序从Amazon SQS 提取此位置并分析视频.视频分析需要大量计算,并且在一天中偶尔会发生.

该网站可根据需求扩展.视频分析应用程序在固定数量的实例上运行.需求高峰在假期期间发生,因此公司 必须在这段时间内向应用程序添加实例.当前使用的所有实例均为按需 Amazon EC2 T2

实例.该公司希望降低当前解决方案的成本. 以下哪个解决方案最符合成本效益?

A:使网站保持在 T2 实例上.确定非高峰时间所需的最少网站实例数,并在使用时使用竞价型实例进行覆盖预留实例以满足高峰需求.将 Auto Scaling 组中的 EC2 R4 和 Amazon EC2 R5 预留实例用于视频分析应用程序.

1. 使网站保持在 T2 实例上.确定非高峰时间所需的最少网站实例数,并使用"预留实例"来覆盖它们,而使用"按需实例"来满足高峰需求.将 Spot Fleet 用于由 Amazon EC2 C4 和 Amazon EC2 C5 竞价型实例组成的视频分析应用程序.
2. 将网站迁移到 AWS Elastic Beanstalk 和 Amazon EC2 C4 实例.确定非高峰时段所需的最少网站实例数,并使用按需实例来覆盖它们,同时使用竞价容量来满足高峰需求.将 Spot Fleet 用于由 C4 和 Amazon EC2 C5 实例组成的视频分析应用程序.
3. 将网站迁移到 AWS Elastic Beanstalk 和 Amazon EC2 R4.实例.确定非高峰时段所需的最少网站实例数,并使用预留实例来覆盖它们,而使用按需实例来满足高峰需求.将 Spot Fleet 用于包含 R4 和 Amazon EC2 R5 实例的视频分析应用程序.

答案: B

Question 180 **12/12考试原题**  **03/09考试原题**

公司拥有一个 Amazon VPC,该 VPC 分为公共子网和私有子网.

Web 应用程序在 Amazon VPC 中运行,并且每个子网都有其自己的 NACL.公共子网的 CIDR 为

10.0.0.0/24.

应用程序负载平衡器已部署到公共子网.专用子网的 CIDR 为 10.0.1.0/24.

在端口 80 上运行Web 服务器的 Amazon EC2 实例将启动到专用子网中.

仅允许应用程序负载平衡器访问 Web 应用程序所需的网络流量在公共子网和私有子网之间传播. 应该编写什么规则集来确保专用子网的 NACL 满足要求? (选择两个.)

A.来自源 0.0.0.0/0 的端口 80 的入站规则.

B.来自源 10.0.0.0/24 的端口 80 的入站规则.

C.端口 80 到目标 0.0.0.0/0 的出站规则.

D.端口 80 到目标 10.0.0.0/24 的出站规则.

E.端口 1024 到 65535 到目标 10.0.0.0/24 的出站规则. 答案: BE

解 释 : https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_Scenario3.html

Question 181 **12/12考试原题**  **03/09考试原题**

公司的 CISO 已要求解决方案架构师重新设计公司的当前 CI / CD 做法,以确保在发现漏洞的情况下尽可能快地在其应用程序中进行补丁程序部署,并且停机时间最少,该公司还必须能够快速滚动支持在发生错误的情况下进行更改.

该 Web 应用程序部署在 Application Load Balancer 后面的Amazon EC2 实例团队中.该公司当前正在使用 Github 托管应用程序源代码,并配置了一个 AWS CodeBuild 项目来构建应用程序.该公司还打算使用AWS CodePipeline 从使用现有 CodeBuild 项目的 Github 提交触发构建.

哪种 CI / CD 配置可以满足所有要求?

1. 使用配置为就地部署的 AWS CodeDeploy 在部署阶段配置 CodePipeline 监视新部署的代码,如果有任何问题,请推送另一个代码更新.
2. 使用为蓝/绿部署配置的 AWS CodeDeploy 在部署阶段配置 CodePipeline 监视新部署的代码,如果有任何问题,请使用 CodeDeploy 触发手动回滚.
3. 使用 AWS Cloudformation 在部署阶段配置 CodePipeline,以创建用于测试和生产堆栈的管道,监视新部署的代码,如果有任何问题,请推送另一个代码更新.
4. 使用 AWS Opsworks 和就地部署在部署阶段配置 CodePipeline.监视新部署的代码,如果有任何问题,

请推送另一个代码更新. 答案: B

Question 182 **12/12考试原题**  **03/09考试原题**

一家公司拥有一个网络应用程序,可将图片和视频安全地上传到 Amazon S3 存储桶.该公司要求仅允许经过身份验证的用户发布内容.该应用程序生成一个预签名 URL,该 URL 用于通过浏览器界面上载对象.大多数用户报告大于 100 MB 的对象的上载时间较慢.

在确保只允许经过身份验证的用户发布内容的同时,Solutions Architect 可以做些什么来提高这些上传的性能?

1. 使用具有资源作为 S3 服务代理的经过边缘优化的 API 终端节点设置 Amazon API Gateway.

为此资源配置 PUT 方法以公开 S3 putobject 操作.使用 COGNITO\_USER\_POOLS 授权者保护 API 网关的安全.让浏览器界面使用 API 网关而不是预先签署的 URL 来上传对象.

1. 使用具有资源作为 S3 服务代理的区域 API 终端节点设置 Amazon API Gateway.为此资源配置 PUT 方法以公开 S3 PutObject 操作使用 AWS Lambda 身份验证器保护 API 网关.让浏览器界面使用 API 网关而不是预先签署的 URL 来上传对象.
2. 在 S3 存储桶上启用 S3 传输加速端点.生成预签名 URL 时使用端点. 让浏览器界面使用 S3 分段上传 Apl 将对象上传到此 URL.
3. 为目标 S3 存储桶配置 Amazon Cloudfront 分发.为 Cloudfront 缓存行为启用 PUT 和 POST 方法.更新Cloudfront 来源以使用 ongin 访问身份(OAI)在存储桶策略中授予 OAI 用户 s3:PutObject 权限.让浏览器界面使用 CloudFront 分发上传对象.

答案: C

Question 183 **12/12考试原题**  **03/09考试原题**

公司的应用程序在 Auto Scaling 组中使用 Amazon EC2 实例.质量保证(QA)部门需要使用大量短期环境来测试应用程序.应用环境当前由部门经理使用 AWS Cloudformation 模板启动.要启动堆栈,管理器使用有权使用 Cloudformation,EC2 和 Auto Scaling API. Manager 希望允许测试人员启动自己的环境,但不想向每个用户授予广泛的权限.

哪个设置可以实现这些目标?

1. 将 AWS Cloudformaton 模板上传到 Amazon S3,让处于质量检查部门权限的用户承担 Manager 的角色,并添加策略以限制对模板及其创建的资源的权限.培训用户从 Cloudformation 控制台启动模板
2. 从环境模板创建一个 AWS Service Catalog 产品.使用现有角色向产品添加启动约束.向 QA 部门的用户授予仅使用 AWS Sevice Catalog API 的权限.训练用户从 AWS Service Catalog 控制台启动模板.
3. 将 AWS Cloudformation 模板上传到 Amazon S3,向 QA 部门的用户授予使用 Cloudformation 和 S3 API 的权限,条件是限制对模板及其创建的资源的权限.训练用户从 Cloudformation 控制台启动模板.
4. 从环境模板创建一个 AWS Elastic Beanstalk 应用程序.授予 QA 部门权限的用户仅使用 Elastic Beanstalk 权限.训练用户使用 Elastic Beanstalk CLI 启动 Elastic Beanstalk 环境,将现有角色作为服务角色传递给环境

答案: B

Question 184

金融服务公司将个性可识别信息记录到其存储的应用程序日志中

在 Amazon S3 中.由于合规性要求,必须在以下位置对日志文件进行加密: 休息.安全团队已要求该公司的本地硬件安全性

模块(HSM)用于生成 CMK 材料.

解决方案架构师应采取哪些步骤来满足这些要求?

1. 创建一个 AWS CloudHSM 集群.使用 AWS\_CloudHSM 作为在AWS KMS 中创建新的 CMK

关键材料的来源以及 AWS-CLOUDHSM 的来源.启用自动按键旋转

在 CMK 上,有效期为 1 年.禁止在日志记录存储桶上配置存储桶策略上载未加密的数据,并要求加密源为 AWS KMS.

1. 供应一个 AWS Direct Connect 连接,确保 RFC 1918 不重叠本地硬件和 VPC 之间的地址空间.在上配置 AWS 存储桶策略

记录桶要求所有对象都是关键材料,并为每个对象创建唯一的 CMK

记录事件.

1. 在 AWS KMS 中创建一个 CMK,没有密钥材料,并且没有 EXTERNAL 的来源.导入密钥使用公钥从本地 HSM 生成的材料导入 CMK 并导入

AWS 提供的令牌.在日志记录存储桶中配置存储桶策略,以禁止上传非加密数据,并且要求加密源为 AWS KMS.

1. 在 AWS KMS 中使用 AWS 提供的密钥材料和 AWS-KMS 的来源创建一个新的 CMK.

禁用此 CMK,并用本地 HSM 中的材料覆盖密钥材料

使用 AWS 提供的公钥和导入令牌重新启用 CMK.启用自动

CMK 上的密钥旋转,持续时间为 1 年.在日志存储桶中配置存储桶策略禁止上传未加密的数据,并要求加密源为 AWS

KMS.

答案: C

Question 185

一个公司有几个团队,每个团队都有自己的 Amazon RDS 数据库,总计 100 TB.该公司正在为商业智能分析师构建数据查询平台,以生成每周业务报告.新系统必须运行临时SQL 查询.

什么是最具成本效益的解决方案

1. 创建一个新的 Amazon Redshift 集群.创建一个 AWS Glue ETL 作业以将数据从 RDS 数据库复制到亚马逊 Redshift 集群中使用 Amazon Redshift 运行查询
2. 创建具有足够核心节点的 Amazon EMR 集群运行 Apache Spark 作业,将数据从 rds 数据库复制到Hadoop 分布式文件系统(HDFS).使用本地 Apache Hive 元存储来维护表定义.使用 Spark SQL 运行查询C.使用 AWS Glue ETL 作业将所有 rds 数据库复制到单个 Amazon Aurora Postgresql 数据库上在Aurora Postgresql 数据库上运行 SQL 查询

D.使用 AWS Glue 搜寻器对所有数据库进行爬网并在 AWS Glue 数据目录中创建表.使用 AWS Glue ETL 作业将数据从 RDS 数据库加载到 Amazon S3,然后使用 Amazon Athena 运行查询.

答案: D

Question 186

公司需要将其本地资源移至 AWS.当前环境由 100 个虚拟机(VMS)组成,总共有 40 TB 的存储.大多数VMS 可以脱机,因为它们仅在工作时间内支持功能,但是有些对任务至关重要.因此必须将停机时间降至最低.

本地网络的管理员为迁移配置了 10 Mbps 的互联网带宽.本地网络吞吐量已达到容量,并且增加成本很高. 解决方案架构师必须设计一个可以在未来 3 个月内执行的迁移解决方案

哪种方法可以满足这些要求?

1. 设置 1 Gbps AWS Direct Connect 连接.然后,提供一个私有虚拟接口,并使用AWS Server 迁移服务

(SMS)将 VMS 迁移到 Amazon EC2

1. 使用 AWS Application Discovery Service 评估每个应用程序,并确定如何使用 AWS 服务或 AWS Marketplace 解决方案重构和优化每个应用程序
2. 从最关键的服务器开始,首先在本地导出 VMS,然后使用 AWS Transfer for SFTP 将每个 VM 导出后安全地上载到 Amazon S3.使用 VM Import / Export 将 VMS 导入 Amazon EC2
3. 使用 AWS SMS 迁移关键的 VM,并在本地导出其他 VM,然后使用 AWS Snowball 将其转移到

Amazone S3.使用 VM Import / Export 将 VM 导入 Amazon EC2

答 案 : D

Question 187 **12/12考试原题** **11/19考试原题**  **03/09考试原题 03/23考题**

公司有一个网站,使用户可以上传视频.公司政策规定,必须对上传的视频进行限制内容分析.将上传的视频 放置在 Amazon S3 中,并将消息连同视频位置一起推送到 Amazon SQS 队列.后端应用程序从 Amazon SQS 提取此位置并分析视频.

视频分析需要大量计算,并且会在一天中偶尔发生.该网站可根据需求扩展.视频分析应用程序在固定数量 的实例上运行.需求高峰在假期期间发生,因此公司这次必须在应用程序中添加实例,所有使用的实例都是 当前的按需 Amazon EC2 T2 实例.该公司希望降低当前解决方案的成本.

以下哪个解决方案最符合成本效益?

1. 使网站保持在 T2 实例上.确定非高峰时段所需的最少网站实例数,并使用竞价型实例来覆盖它们,同时使用预留实例来满足高峰需求.将 Auto Scaling 组中的Amazon EC2 R4 和 Amazon EC2 R5 预留实例用于视频分析应用程序
2. 使网站保持在 T2 实例上确定高峰时段需要的最少网站实例数量,并使用预留实例来覆盖它们,而使用按需实例来满足高峰需求.将 Spot Fleet 用于由 Amazon EC2 C4 和 Amazon EC2 C5 竞价型实例组成的视频分析应用程序
3. 将网站迁移到 Aws Elas Beanstalk 和 Amazon EC2 C4 实例确定非高峰时段需要的网站实例的最小数量,并使用按需实例来覆盖它们,同时使用竞价容量来满足高峰需求,使用 Spot Fleet 来满足需求视频分析应用程序由 C4 和 Amazon EC2 C5 立场组成
4. 将网站迁移到 Aws Elas Beanstalk 和 Amazon EC2 C4 实例确定非高峰时期需要的网站实例的最小数量,并使用预留实例来覆盖它们,而使用按需实例来满足高峰需求,使用 Spoor Fleet 由 R4 和 Amazon EC2 R5 实例组成的视频分析应用程序.

答案: B

Question 188

尽管没有报告显示用户看到错误页面,但是随着用户群的增加,公司的主要 Intranet 页面的响应时间会降低.该应用程序以只读模式使用 Amazon Dynamodb.

即使在用户报告性能下降期间,成功请求的 Amazon DynamoDB 延迟指标也处于稳定状态.开发团队已将问题与执行扫描和读取操作时应用程序日志中的 ProvisionedThroughputexceeded 异常相关联.该团队还确定了一组分散的单个数据项上读取活动稳定增长的访问模式.首席技术官希望改善用户体验.

只需对应用程序进行最少的更改,哪些解决方案将满足这些要求?(选择两个)

1. 更改 dynamodb 表的数据模型,以确保所有扫描和读取操作均符合Dynamodb 统一数据访问的最佳做法,从而达到为 Dynamodb 表提供的全部请求吞吐量.
2. 启用 Dynamodb 自动缩放功能,以在表流量增加时管理吞吐量.设置上限和下限以控制成本,并根据峰值使用量和流量变化速度来设置目标使用率.
3. 在启用集群模式的情况下为 Redis 设置 Amazon Elasticache.应该为群集配备足够的分片,以分散应用程序负载,并为每个分片至少提供一个只读副本节点.
4. 实现 Dynamodb Accelerator(DAX)客户端,并为 DAX 群集提供适当的节点类型,以维持应用程序负载. 调整项目和查询缓存配置以获得最佳用户体验
5. 在应用程序代码中删除错误重试和指数退缩以处理节流错误 答案: BD

Question 189

一家公司在使用 Amazon API Gateway,Amazon Lambda 和 Amazon Dynamodb 的新部署的无服务器基础架构方面遇到问题.

在稳定状态下,应用程序按预期运行.但是,在高峰负载期间,需要数以万计的同时调用,并且用户请求在成 功之前会多次失败.二进制文件检查了每个组件的日志,特别侧重于 Lambda 的 Amazon Cloudwatch 日志. 服务或应用程序没有错误日志记录.

是什么导致此问题?

1. Lambda 分配的内存非常低,这导致该功能在峰值负载时失败
2. Lambda 位于使用 nat 网关连接到 Internet 的子网中,该功能实例在VPC 中没有足够的 Amazon EC2

资源以适应负载扩展

1. 在 API 网关上设置的油门限制非常低.在高峰负载期间,其他请求不会传递给 lambda.
2. Dynamodb 设置为自动缩放模式.在峰值负载期间,Dynamodb 会在后台调整容量和吞吐量,这会导致暂时的停机.缩放完成后,重试成功完成

答案: C

第 190 题

一家公司最近将其旧版基础架构配置脚本转换为 AWS Cloudformation 模板.新开发的模板托管在公司的私有 Github 存储库中.自采用 Cloudformation 以来,该公司在 Cloudformation 模板的更新方面遇到了多个问题,导致执行失败或创建不稳定的环境.管理人员因错误增加而感到担忧,并要求解决方案架构师设计对 Cloudformation 模板更新的自动化测试.

解决方案架构师应该怎么做才能满足这些要求?

1. 使用 AWS Codepipeline 从私有 Github 存储库中存储的 Cloud Formation 模板创建变更集.使用 AWS Code Deploy 执行变更集.包括 Codepipelineaction 以使用AWS Code 运行的测试脚本测试部署,以构建云形成模板并执行它,并执行 Code Deploy 使用 AWS Codebuild 运行的测试脚本测试部署.
2. 使用 AWS Lambda 将 Github 存储库镜像到Aw Code Commit.使用 AWS Code Deploy 从 Code build

创建更改集

1. 使用 AWS Code Pipeline 从私有 Github 存储库中存储的 Cloud Formation 模板创建并执行更改集.配置代码管道操作以使用 AWS Codebuild 运行的测试脚本来测试部署
2. 使用 AWS Lambda 将 Github 存储库镜像到 AWS Code Commit 使用 AWS Code Build 从

Cloudformation 模板创建变更集并执行,让 Codebuild 使用测试脚本测试部署

答案: C

Question 191 **12/12考试原题**  **03/09考试原题**

一家企业公司希望为其 AWS 组织中的所有账户实施成本控制,并启用了全部功能.该公司已将组织单位(OU)映射到其业务单位,并且它希望针对这些业务单位的个人 AWS 支出进行计费.该公司的 AWS 账单最近出现了激增,这引起了财务团队的关注.解决方案架构师需要在设计解决方案的过程中调查出现高峰的原因,该解决方案将跟踪组织中的AWS 成本,并在业务部门的成本超过特定货币阈值时向所需团队生成通知.

哪种解决方案可以满足这些要求?

1. 使用成本资源管理器解决附加费用的原因.设置 AWS Lambda 函数以通过 OU 中的每个 AWS 账户监视公司的 AWS 账单.由金融团队在 AWS Systems Manager 参数存储中设置的阈值金额.在 L mbda 函数中编写自定义规则,以验证AWS 账户的任何隐藏成本.超出预算阈值时,将 Lambda 函数的通知触发到Amazon SNS 主题.
2. 使用 AWS Trusted Advisor 对额外费用的原因进行故障排除.设置 AWS Lambdafunction 来监视 OU 中每个 AWS 账户的公司 AWS 账单.在 AWS Systems Manager 参数存储中存储阈值金额财务团队.在Lambda 函数中编写自定义规则,以验证 AWS 账户的任何隐藏成本.超出预算阈值时,使用 Amazon SNS 从 Lambda 函数触发一封电子邮件给所需团队
3. 使用 Cost Explorer 排查额外费用的原因.通过将链接的帐户分组,使用 AWS 预算和财务团队为每个

OU 设置的金额创建预算,通过将 Amazon SNS 通知配置到预算中所需的团队来进行配置.

1. 使用 AWS Trusted Advisor 对额外费用的原因进行故障排除.使用 Aws 预算创建一个预算,并通过财务链接小组对每个 OU 的分组来设置财务金额.添加要在公司中用作预算过滤器的 Amazon EC2 实例类型. 通过为财务团队电子邮件地址订阅配置 Amazon SNS 主题,以接收预算通知.

答案: C

Question 192

一家公司使用 AWS Cloudformation 模板为其用户提供 AWS 解决方案.用户在其帐户中启动模板,以为其配置不同的解决方案.用户希望在保留以下功能的同时改善解决方案的部署策略:

-为自己的特定部署将自己的功能添加到解决方案中

-对更改进行单元测试

-打开和关闭功能以进行部署.

-通过代码更改自动更新.

-运行安全扫描工具进行部署

解决方案架构师应使用哪些策略来满足要求?

1. 允许用户将解决方案代码下载为 Docker 映像.将 AWS Codebuild 和 AWS Codepipeline 用于 CI / CD 管道.将 Docker 映像用于不同的解决方案功能,并使用 AWS CLI 开启和关闭功能.使用 AWS Codedeploy 来运行单元测试和安全扫描,以及用于部署和更新具有更改的解决方案.
2. 允许用户下载解决方案代码工件.将 AWS Codecommit 和 AWS Codepipeline 用于 CI / CD 管道.将AWS Amplify 插件用于不同的解决方案功能和用户提示以启用或禁用功能.使用 AWS Lambda 运行单元测试和安全扫描,并使用 AWS Codebuild 部署和更新具有更改的解决方案
3. 允许用户在其 Amazon S3 存储桶中下载解决方案代码工件.将 Amazon S3 和 AWS Codepipeline 用于 CI / CD 管道.将 Cloudformation 堆栈集用于不同的解决方案功能,以及打开和关闭功能.使用 AWS Lambda 运行单元测试和安全扫描,并使用 Cloudformation 部署和更新具有更改的解决方案
4. 允许用户下载解决方案代码工件将 AWS Code Commit 和 AWS Codepipeline 用于 CI / CD 管道对不同的解决方案功能使用 AWS Cloud Development Kit 构造,并使用清单文件打开和关闭功能.使用 AWS Codebuild 运行单元测试和安全扫描,以及部署和更新具有更改的解决方案

答案: D

Question 193

一家公司正在运营一个大型的客户服务呼叫中心,并使用自定义应用程序来存储和处理呼叫记录,出于质量保证的目的,离岸团队抄录了大约 2%的呼叫记录.这些录音最多需要 72 个小时才能被转录.记录存储在NFS 共享上,然后在 90 天后存储到异地位置.该公司使用 Linux 服务器来处理呼叫记录和管理转录队列. 质量保证人员还可以使用该应用程序对通话记录进行查看和评分.

该公司计划将系统迁移到 AWS,以降低存储成本和转录呼叫所需的时间.

应该采取哪些行动来达到公司的目标?

1. 将呼叫记录从呼叫中心上传到 Amazon S3.设置 S3 生命周期策略,以在 90 天后将通话记录移至Amazon S3 Glacier.使用 AWS Lambda 触发器通过 Amazon Transcribe 转录呼叫记录.使用 Amazon S3,Amazon AP 网关和 Lambda 托管那里的视图和计分应用程序.
2. 将呼叫记录从呼叫中心上传到 Amazon S3.设置 S3 生命周期策略,以在 90 天后将通话记录移至Amazon S3 Glacier.使用 AWS Lambda 触发器通过 Amazon Mechanical Turk 转录通话记录.在Application Load Balancer 后面的 Auto Scaling 组中使用 Amazon EC2 实例来托管审阅和评分应用程序. C.在应用程序负载平衡器后面的 Auto Scaling 组中使用 Amazon EC2 实例托管视图和计分应用程序从呼叫中心将呼叫记录上传到此应用程序并将其存储在 Amazon EFS 挂载点上. 90 天后使用 AWS

Backup 存档呼叫记录,然后使用 Amazon Transcribe 记录呼叫记录.

D.从队列将通话录音上传到 Amazon S3.设置 S3 生命周期策略,以在 90 天后将通话记录移至 Amazon S3 Glacier.在 Auto Scaling 组中使用 Amazon EC2 实例,将记录发送到 Amazon Mechanical Turk.forranscnption 使用队列中的对象数作为缩放指标.使用 Amazon S3,Amazon APIGateway 和 AWS Lambda 托管审阅和计分应用程序

答案: A

Question 194

解决方案架构师正在构建一个将在 AWS 中运行的容器化 NET Core 应用程序

Fargate 应用程序的后端需要具有高可用性的 Microsoft SQL Server 所有应用程序层必须高度可用用于连接字符串的凭据

SQL Server 不应存储在.NET Core 前端容器内的磁盘上. 解决方案架构师应使用哪些策略来满足这些要求?

1. 设置 SQL Server 以通过Service Auto Scaling 在 Fargate 中运行.创建一个 Amazon ECS 任务执行角色,该角色允许 Fargate 任务定义获取在 Fargate 中运行的 SQL Server 凭证的秘密值.在 Fargate 任务定义的 secrets 部分中,在 AWS Secrets Manager 中指定密钥的 ARN,以便当环境变量构造连接字符串时,

可以将敏感数据注入到容器中.设置了. NET Core 服务在启动时用于读取应用程序,以在多个可用区域中的应用程序负载均衡器后面自动进行服务扩展

1. 在 Amazon RDS 上创建 SQL Server 的 Multi-az 部署.在 AWS Secrets Manager 中为 RDS 数据库的凭证创建密钥.创建一个 Amazon ECS 任务执行角色,该角色允许 Fargate 任务定义获取 Secrets Manager 中 RDS 数据库的凭证的秘密值.在 Fargate 任务定义的 secrets 部分中,在 Secrets Manager 中指定密钥的 ARN,以便可以在启动时将敏感数据作为环境变量注入到容器中,以读取到应用程序中以构造连接字符串.在多个可用区中的应用程序负载均衡器后面使用服务自动缩放的 Fargate
2. 创建一个 Auto Scaling 组以在 Amazon EC2 上运行 SQL Server.在 AWS Secrets Manager 中为在EC2 上运行的 SQL Server 的凭据创建密钥.创建一个 Amazon ECS 任务执行角色,以允许 Fargate 任务定义获取 EC2 上 SQL Server 凭据的机密值在 Fargate 任务定义的 secrets 部分中,在 Secrets Manager 中指定密钥的 ARN,以便可以注入敏感数据在启动时将其作为环境变量放入容器中,以读取应用程序以构造连接字符串. NET Core 服务在多个可用区中的应用程序负载均衡器后面使用服务自动缩放
3. 在 Amazon RDS 上创建 SQL Server 的 Multi-az 部署.在 AWS Secrets Manager 中为 RDS 数据库的凭证创建密钥.在 Fargate 任务定义中为 NET Core 容器创建非持久空存储,以存储敏感信息.创建一个Amazon ECS 任务执行角色,该角色允许 Fargate 任务定义获取Secrets Manager 中 RDS 数据库的凭证的秘密值.在 Fargate 任务定义的"机密"部分中,在"机密管理器"中指定机密的 ARN,可以将敏感数据写入机密. NET Core 服务在多个可用性驱动器中的 Aplication Load Balancer 后使用 Serivce Auto Scaling

答案: B

Question 195 **03/23考题**

公司在 VPC 内部具有内部 AWS Elastic Beanstalk 工作者环境,该环境必须访问公共 Internet 上 HTTPS 终端节点上可用的外部支付网关 API.由于安全策略的原因,支付网关应用程序团队只能授予对一个公共IP 地址的访问权限

哪种体系结构将设置一个 Elastic Beanstalk 环境来访问公司的应用程序,而无需在公司端进行多次更改? A.配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在私有子网中,并具有到公共子网中 NAT

网关的出站路由.将弹性 IP 地址与可以在支付网关应用程序端列入白名单的 NAT 网关相关联.

1. 配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在具有 Internet 网关的公共子网中.将弹性 IP 地址与可以在支付网关应用程序端列入白名单的 Internet 网关相关联
2. 配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在专用子网中.设置 HTTPS\_PROXY 应用参数,以将出站 HTTPS 连接发送到部署在公共子网中的 EC2 代理服务器.将弹性IP 地址与EC2 代理主机相关联,该主机可以在付款网关应用程序端白名单列出
3. 配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在公共子网中.设置 HTTP\_SPROXY 和NO\_PROXY 应用程序参数以将非 vpc 出站 HTTPS 连接发送到部署在公共子网中的 EC2 代理服务器.将弹性 IP 地址与可以在支付网关应用程序端列入白名单的EC2 代理主机相关联

答案: A

说明:https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/vpc.html

Question 196

解决方案架构师正在构建用于更新由 Web 服务器启动的用户元数据的解决方案.该解决方案需要在不到30 秒的时间内迅速将数百个工作扩展到成千上万个工作.这些服务器必须是异步的,始终可用,并且可以最大程度地降低成本.

解决方案架构师应使用哪些策略来满足这些要求?

1. 创建一个将更新用户元数据的 AWS SWF 工作程序更新 Web 应用程序以为每个作业启动一个

newworklow

1. 创建一个将更新用户元数据的 AWS Lambda 函数.创建一个 Amazon SQS 队列,并将其配置为

Lambda 函数的事件源.更新 Web 应用程序以将作业发送到队列

1. 创建一个将更新用户元数据的 AWS Lambda 函数.创建将触发 Lambda 函数的AWS Step Functions.

更新 Web 应用程序以为每个作业启动 Step Functions

1. 创建一个 Amazon SQS 队列.与工作人员一起创建 AMI,以检查队列并更新使用元数据.使用新的 AML

配置 Amazon EC2 Auto Scaling 组更新 Web 应用程序以将作业发送到队列答案: B

Question 197 **12/12考试原题**

一家公司正在从本地迁移到 AWS,并且刚刚部署了在 Linux 上运行的第一组应用程序.该公司将继续从本地主机到 AWS 进行流量维护.该公司希望降低解决方案的成本,并逐步将其全部工作负载迁移到 AWS. 哪种解决方案可以满足这些要求?

1. 在本地和 VPC 之间建立 VPN 连接.创建 IAM 角色和权限以启用 AWS Systems Manager Session Manager.安装 Systems Manager 代理并启用 Systems Manager.根据策略限制创建 IAM 用户和标签
2. 在本地和 VPC 之间建立 VPN 连接.使用 Amazon EC2 控制台创建密钥对.使用密钥对部署 EC2 实例对于本地实例,请部署与密钥对匹配的公钥.
3. 在本地和 VPC 之间建立 AWS Direct Connect.创建 IAM 角色和权限以启用 AWS Systems Manager Session Manager.安装 Systems Manager 代理并启用 Systems Manager.根据策略限制创建 IAM 用户和标签
4. 在本地和 VPC 之间建立 AWS Direct Connect.配置一个 Ipsec 隧道.创建 IAM 角色和权限以启用 AWS Systems Manager 会话管理器,安装 System Manager 代理和 eable Systems Manager,并根据重复限制创建 IAM 用户和标签.

答案: A

Question 198

解决方案架构师需要设计一个可用的应用程序,即使存在潜在的故障,该应用程序也允许经过身份验证的 用户保持与应用程序的连接.

哪种解决方案可以满足这些要求?

1. 在 Amazon EC2 实例上部署应用程序使用 Amazon Route 53 将请求转发到 EC2 实例使用 Amazon Dynamodb 保存经过身份验证的连接详细信息
2. 在 Auto Scaling 组的 Amazon EC2 实例上部署应用程序.在 hande 请求上使用面向 Internet 的

Application Load 10 Balancer.使用 Amazon Dynamodb 保存经过身份验证的连接详细信息

1. 在 Auto Scaling 组的 Amazon EC2 实例上部署应用程序.在前端使用面向 Internet 的应用程序负载均衡器使用 EC2 实例保存经过身份验证的连接详细信息
2. 在 Auto Scaling 组的 Amazon EC2 实例上部署应用程序.在前端使用面向 Internet 的应用程序负载平衡器使用托管 MYSQL 数据库的 EC2 实例保存经过身份验证的连接详细信息

答案: B

Question 199

解决方案架构师正在为公司即将推出的新应用程序设计数据存储和检索体系结构.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,需要存储在一个持久的位置,以便

可以以低延迟对其进行检索.数据是临时数据,公司仅需将数据存储 120 天,然后才能删除数据.

解决方案架构师计算得出,在一年的过程中,存储需求约为 10-15 TB.

哪种存储策略最符合设计要求的成本效益?

1. 设计应用程序以将每个传入记录存储为单个. Amazon S3 存储桶 toa 生命周期策略中的 CSV 文件可删除 120 天以上的数据
2. 将应用程序设计为将每个传入记录存储在已针对规模正确配置的 Amazon Dynamodb 表中,使用

Dynamodb 的生存时间(TTL)功能删除超过 120 天的记录.

1. 设计应用程序以将每个传入记录存储在 Amazon RDS MySQL 数据库的单个表中,运行每晚 cron 作业, 然后执行查询以删除 120 天以上的任何记录顺序
2. 设计应用程序以在将传入记录写入 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

Question 200

一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 帐户结构,并且在每个组织单位(OU)中都有一个将由采购经理使用的简短服务帐户,采购团队的政策表明开发人员应能够获取第三方软件如果要从满足条件的 AWS Marketplace 中只有一个经过批准的列表" Private Marketplace"中实现此要求,采购团队希望将" Private Marketplace"的管理限制为角色用户,组,roies 和公司中的帐户管理员,应拒绝" Private Marketplace"的管理访问权限.

设计满足这些要求的体系结构的最有效的方法是什么?

1. 在组织中的所有 AWS 账户中创建一个名为采购经理角色的 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 帐户中的所有 IAM 用户和角色,以拒绝对Awsprivatemarkeplaceadminfullaccess 托管策略的权限.
2. 在组织中的所有 AWS 帐户中创建一个名为采购经理角色的 IAM 角色.将管理员访问受管策略添加到角色.使用 Awsprivatemarketplace Access 托管策略定义权限边界,并将其附加到所有开发人员角色
3. 在组织中的所有共享服务帐户中创建一个名为采购经理角色的 IAM 角色将Awsprivatemarketplaceadminfulaccess 托管策略添加到该角色.创建组织根级别的 SCP,以拒绝对每个人(名为"采购经理角色")的角色进行管理私有市场的权限.创建另一个组织的根级别 SCP,以拒绝创建该组织中每个人的 IAM 角色,名为采购采购经理角色
4. 在将由开发人员使用的 AWS 账户中创建一个名为 Purchase-manager-role 的 IAM 角色.将Awsprivatemarketplaceadminfullaccess 托管策略添加到角色.在组织中创建一个 SCP,以拒绝向所有人管理私有市场的权限,但名为采购经理角色的角色除外将 SCP 应用于组织中的所有共享服务帐户

答:C

Question 201

公司有一个在 AWS 上运行的内部应用程序,该应用程序用于跟踪和处理公司仓库中的货物.当前,系统收到订单后,会通过电子邮件向工作人员发送运送包裹所需的信息.包裹寄出后,工作人员会回复电子邮件,并 将订单标记为已寄出.该公司希望停止在应用程序中使用电子邮件,并转向无服务器应用程序模型

哪种架构解决方案可以满足这些要求?

1. 使用 AWS Batch 来配置运送包裹所需的不同任务.让 AWS Batch 触发一个 AWS Lambda 函数,该函数创建并打印运输标签.扫描完该标签后,当标签离开仓库时,让另一个 Lambda 函数将流程移至 AWS Batch 作业的下一步
2. 创建新订单后,将订单信息存储在 Amazon SQS 中,让 AWS Lambda 每 5 分钟检查一次队列并处理所有需要的工作.需要运送订单时,请 Lambda 在仓库中打印标签.扫描完标签(离开仓库后)后,请对 Amazon EC2 实例进行更新 Amazon SQS
3. 更新应用程序以在 Amazon Dynamodb 中存储新订单信息.创建新订单时,触发 AWS Step Functions 工作流将订单标记为"进行中",然后将包装标签打印到仓库.标签被扫描并完成后,应用程序将触发 AWSL ambda 函数,该函数会将订单标记为已发货并完成工作流程
4. 在 Amazon EFS 中存储新订单信息让实例从NFS 中提取新信息,并将该信息发送到仓库中的打印机. 扫描完标签(标签离开仓库后)后,让 Amazon API Gateway 调用实例以从Amazon EFS 中删除订单信息

答 案 :C Question 202

一家制造公司正在成倍增长,并已获得资金来改善其 IT 基础架构和电子商务的存在.

该公司的电子商务平台由静态资产组成,这些静态资产主要由存储在Amazon s3 Amazon Dymamodb 表中的产品图像组成,这些表存储产品信息,用户信息和订单信息包含在 Elastic Load Balancer 后面的应用程序前端的 Web 服务器该公司希望设置灾难恢复网站位于单独的区域中.

解决方案架构师应在满足所有要求的同时采取哪种行动组合来实施新设计?(选择三项)

1. 启用 Amazon Route 53 运行状况检查以确定主站点是否关闭,并在出现问题时将流量路由到灾难恢复站点
2. 在包含静态资产的存储桶上启用 Amazon S3 跨区域复制
3. 在 Elastic Load Balancer 上启用多区域目标并在两个区域中均目标Amazon EC2 实例
4. 启用 Dynamodb 全局表以实现多区域表复制
5. 启用 Amazon Cloudwatch 并创建 Cloud Watch 警报,以在应用程序延迟超过所需阈值时将流量路由到灾难恢复站点

答:ABD

Question 203

客户拥有一个网站,其中显示了整个市场上所有可用的交易.该站点通常承受 5 个大型 EC2 实例的负载. 但是,在感恩节假期的前一周,他们遇到了将近 20 个大型实例的负载.该时间段内的负载会根据办公时间在一天中变化.

以下哪种解决方案具有成本效益,并且可以帮助网站实现 更好的性能?

1. 设置为在预假期期间运行 10 个实例,并且仅在办公时间内进行扩展通过使用 AutoScaling 时间表启动另外 10 个实例.
2. 在办公时间内,每天仅运行 10 个实例,并手动启动 10 个实例.
3. 在休假前设置 20 个实例以使其连续运行.
4. 在休假前设置一个方案,其中组织有 15 个实例在运行

根据网络 I / O 策略使用 Auto Scaling 扩展和缩减 5 个实例.

答:A

说明:

AWS 提供了随需应变的可扩展基础架构. AWS EC2 允许用户启动按需实例,并且组织应创建正在运行的实例的 AMI.当组织遇到不同的负载并且负载的时间未知(但是它比常规流量高)时,建议组织先启动一些实例,然后根据策略设置 AutoScaling 的大小来进行扩展和缩减. EC2 指标,例如网络 I / O 或 CPU 利用率.如果组织将所有其他 10 个实例保留为 AutoScaling 策略的一部分,有时会在突然增加负载的情况下启动,

实例,可能无法提供最佳性能.因此,出于成本效益的考虑,建议组织根据 AutoScaling 策略让其他 5 个实例继续运行,并计划接下来的 5 个实例继续运行.

Question 204

一队 Amazon ECS 实例用于轮询 Amazon SQS 队列并更新 Amazon Dynamodb 数据库中的项目.表中的项目未更新,并且 SQS 队列已满.尝试更新表时,Amazon Cloudwatch 日志显示一致的 400 错误.所配置的写容量单位已适当配置,并且没有发生节流.

故障的可能原因是什么?

答:ecs 服务已删除

1. ECS 配置不包含 Auto Scaling 组
2. 修改 ECS 实例任务执行 IAM 角色
3. 修改 ECS 任务角色答案:D

Question 205

一家公司最近将其旧版基础架构配置脚本转换为 AWS Cloudformation 模板.新开发的模板托管在公司的私有 Github 存储库中.自从采用 Cloud Formation 以来,该公司在 CloudFormation 模板的更新上遇到了多个问题,导致执行失败或创建不稳定的环境,管理层对错误的增加感到担忧,并要求解决方案架构师设计Cloudformation 模板更新的自动化测试.

解决方案架构师应怎么做才能满足这些要求?

1. 使用 AWS Code Pipe 从存储在私有Github 存储库中的 Cloudformation 模板创建变更集.使用 AWS Code Deploy 执行变更集.包括一个代码管道操作,以使用由 AWS Code Build 运行的测试脚本来测试部署.
2. 使用 AWS Lambda 将 Github 存储库镜像到AWS Code Commit.使用 AWS Code Deploy 从Cloudformation 模板创建更改集并执行它.让 Codedeploy 使用 Aws Code 构建运行的测试脚本来测试部署.
3. 使用 AWS Code Pipeline 从存储在私有 Github 存储库中的 Cloud Formation 模板创建并执行更改集, 配置 Code Pipeline 操作以使用 AWS Codebuild 运行的测试脚本来测试部署
4. 使用 AWS Lambda 将 Github 存储库镜像到 AWS Code Commit.使用 Aws Code Build 从

Cloudformation 模板创建一个变更集并执行它,以使用测试脚本让 Code Build 测试专家答案:C

Question 206  **03/09考试原题**

一家公司正在内部环境中托管三层 Web 应用程序.由于最近的激增命令了流量,从而导致停机和严重的财务影响,因此该公司应将应用程序割礼给 Aws,该应用程序是用 NET 编写的,并且依赖于 aMYSQL 数据库. 解决方案架构师必须设计一种可扩展且高度可用的解决方案,以满足每天 200,000 用户的需求.

设计师应该采取哪些步骤来设计合适的解决方案?

1. 使用 AS Elastic Beanstalk 通过 Web 服务器环境和 AmazonRDS MYSQL Multi AZ 数据库实例创建新应用程序.该环境应在多个可用区中启动网络负载均衡器(Amazon EC2 Auto Scaling 组的 NLBINfront.使用 Amazon Route 53 aliasecord 将流量从公司域路由到 NLB
2. 使用 AWS Cloudformation 在包含三个可用区的 Amazon EC2 Auto Scaling 组的前面启动一个包含应用程序负载均衡器(ALB)的堆栈.堆栈应使用保留删除策略启动 Amazon Aurora MYSQL DB 集群的Multi-az 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 创建自动缩放的 Web 服务器环境,该环境跨越具有跨区域的 Amazon Aurora MYSQL DB 集群的多重(ALB)ina 多部署部署读取地理邻近性郊游策略以在两个区域之间路由流量路由 53
4. 使用 AWS Cloudformation 在包含三个可用区的竞价型实例的 Amazon ECS 集群之前启动包含应用程序负载平衡器(ALB)的堆栈.堆栈应启动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 :B

Question 207 **03/09考试原题**

一家公司正在 AWS 上迁移其应用程序.这些应用程序将部署到业务部门拥有的 AWS 账户中.该公司有几个开发人员团队,他们负责

开发和维护所有应用程序,该公司期望用户数量快速增长. 公司的首席技术官具有以下要求

-开发人员必须使用 AWS Cloudformation 启动 AWS 基础设施

-开发人员必须不能在 Cloud Formation 之外创建资源

-解决方案必须能够扩展到数百个 AWS 账户； 以下哪项符合要求? (选择两个)

1. 使用 Cloudformation 创建一个 IAM 角色,该角色可以由 Cloud Formation 承担,该角色具有创建通用需求的所有资源的权限,使用 Clodformation 堆栈集将此模板部署到每个 AWS 账户
2. 在中央帐户中,创建一个可由开发人员承担的 IAM 角色,并附加一个允许与 Cloudformation 进行交互的策略.修改"假定策略文档"操作以使 LAM 传递给 Cloudformation
3. 使用云形成,创建开发人员可以承担的 IAM 角色,并附加允许与角色交互并传递角色的策略.附加内联策略以拒绝访问所有其他 AWS 服务.使用 Cloudformation Stack Set 将此模板部署到每个 As 帐户
4. 使用 Cloud Fommaon,为每个开发人员创建一个 IAM 角色,并附加允许与 Cloudformation 进行交互的策略使用 Cloud Formaton Stack Set 将这个模板部署到每个 Awsaccount
5. 在一个中央 AS 帐户中,创建一个 IAM 角色,由 Cloud Formation 承担,该角色有权创建公司所需的资源. 创建允许 IAM 角色管理资源的 Cloud Formation 堆栈策略使用 Cloudformation 堆栈集将Cloudformation 堆栈策略部署到每个 AWS 账户

答:AE

Question 208

在审核期间,安全团队发现开发团队正在将 IAM 用户秘密访问密钥放入其代码中,然后将其提交到 AWS ode Commit 存储库.

安全团队希望自动查找和修复其安全漏洞的实例哪种解决方案将确保自动对凭据进行适当保护?

1. 使用 Aws 系统管理器,每晚运行脚本,运行 ommand 来搜索开发实例上的凭据.如果找到,请使用 AWS Secrets Manager 旋转凭证
2. 使用预定的 AWS Lambda 函数从代码提交下载和扫描应用程序代码如果找到凭证,请生成新凭证并将其存储在 AWS KMS 中
3. 配置 Amazon Macie 扫描代码提交存储库中的凭证.如果找到凭证,则触发 AWS Lambda 函数以禁用凭证并通知用户
4. 配置代码提交触发器以调用 AWS Lambda 函数以扫描新代码提交以获取凭证.如果找到凭证,请在

AWS IAM 中禁用它们并通知用户. 答案:D

Question 209

公司当前将数据托管在 IBM Db2 数据库中. Web 应用程序调用在数据库上运行存储过程的 AP 来检索只读的用户信息数据.该数据本质上是历史数据,每天都在变化.当用户登录到应用程序时,需要在 3 秒内检索其数据.用户每登录一次,存储过程就会运行.用户每天登录几次以查看股票价格.由于 Db2 CPU 许可,运行此数据库已成为成本禁止.绩效目标未实现.由于长时间运行的队列,Db2 中的超时很常见.

解决方案架构师应采用哪种方法将此解决方案迁移到 AWS?

1. 在 Amazon Fargate 中重新托管 Db 数据库迁移所有 e 数据在 Fargate 中启用缓存.重构 API 以使用

Fargate Db2 数据库实现 Amazon API Gateway 并启用 API 缓存.

1. 使用 AWS DMS 通过连续复制任务将数据迁移到 Amazon Dyamodb.重构 API 以使用 Dynamodb 数据.在 Amazon API Gateway 中实现重构的 API 并启用 API
2. 在大型机上创建本地缓存以存储查询输出.每天使用 SFTP 同步到Amazon S3.重构 API 以使用

Amazon EFS.实现 Amazon API Gateway 并启用 API 缓存.

1. 每天提取数据并将数据复制到 AWS Snowball 以存储在 Amazon S3 上.每天同步,重构 API 以使用 S3

数据,实施 Amazon API Gateway 并启用 API 缓存答:B

Question 210

解决方案架构师正在设计应用程序层的部署策略,并具有以下要求.

-在应用程序启动之前,应用程序代码将需要 500 GB 静态数据集.

-应用层必须能够根据需求扩展和缩减,并且启动时间尽可能短.

-开发团队应该能够每天多次更新代码.

-必须在发布的 48 小时内安装关键操作系统(OS)补丁. 哪种部署策略可以满足这些要求?

1. 使用 AWS Systems Manager 创建具有更新的 OS 补丁程序的新 AMI.更新 autoScaling 组以使用修补的 AMI 并替换现有的未修补实例,使用 Aws CodeDeploy 将应用程序代码推送到实例.将静态数据存储在Amazon efs 中.
2. 使用 Aws Systems Manager 创建具有更新的 OS 修补程序的新AMI.更新 auto Scaling 组以使用修补的 AMI 并替换现有的未修补实例.每天晚上以批处理作业的方式更新 os 补丁和应用程序代码.将静态数据存储在 Amazon EFS 中.
3. 将 Amazon 提供的 AMI 用于 os 配置将 Auto Scaling 组设置为静态实例计数.配置 Amazon EC2 用户数据脚本以从 Amazon S3 下载数据.发行时,请使用Aws Systems Manager 安装 os 修补程序.使用 Aws Code Deploy 将应用程序代码推送到实例.
4. 为操作系统使用 Amazon 提供的 AMI.配置一个 Auto Scaling 组.配置 Amazon EC2 用户数据脚本以从Amazon S3 下载数据.在每个更新的 Amazon 提供的 AMI 版本之后,替换现有实例.使用 AWS Code Deploy 将应用程序代码推送到实例.

答 :A Question 211

拥有数百个 AWS 账户的大型公司拥有新建立的集中式内部流程,用于购买新的或修改现有的预留实例.此过程要求所有想要购买或修改预留实例的业务部门将请求提交给专门的团队以进行采购或执行.以前,业务部门将直接在其各自的 AWS 账户中直接购买或修改 ReservedInstances.

应该采取哪种步骤组合才能以最安全的方式主动执行新流程?

答.确保所有 AWS 账户均属于以所有功能模式运行的 Aws Organizations 结构的一部分

1. 使用 AWS Config 报告拒绝访问 ec2:Purchase Reservednstancesoffering 和 ec2:Modify ReservationInstances 操作的IAM 策略的附件.
2. 在每个 AWS 账户中,为 ec2 购买预留实例产品和 ec2:修改预留实例操作创建一个带有拒绝规则的 IAM

策略.

1. 创建一个包含对 ec2 的拒绝规则的 Scp:购买 ReservedInstances 产品和ec2Modify ReservedInstances 操作.将 SCP 附加到 Aws Organizations 结构的每个组织单位(ou).
2. 确保所有 AWS 账户都属于以合并计费功能模式运行的 AWS Organizations 结构的一部分答:AD

Question 212

一家金融服务公司正在迁移到 AWS,并希望使开发人员能够进行实验和创新,同时阻止访问生产应用程序.

公司有以下要求:

-生产工作负载无法直接连接到互联网.

-必须将所有工作负载限制在 us-west-2 和 eu-central-1 地区

-当 Developersandboxes 每月在 AWS 上的支出超过 500 美元时,应发送通知. 创建符合公司要求的多帐户结构需要采取哪种行动组合? (选择三个)

1. 在 AWS Organizations 中为组织内的每个生产工作负载创建帐户.将生产帐户放在组织单位(OU)中.对于每个帐户,删除默认的 VPC.创建一个"拒绝"规则的 SCP,以连接 Internet 网关并创建默认的 VPC 操作. 将 SCP 附加到生产帐户的 ou.
2. 在 AWS Organizations 中为组织内的每个生产工作负载创建帐户.将生产帐户放置在组织单位(OU)中. 在 Attach aninternet 网关操作上创建带有拒绝规则的 SCP,以阻止使用默认 VPC 的情况下,创建带有拒绝规则的 SCP.将 SCPS 附加到生产帐户的 ou.
3. 在 aus RequestedRegion 条件键上使用 us-west-2 和 eu-central-1 值创建一个包含 StringNotEquals

条件的 Cloudfront:\* iam:\*,route53:\*和 support:\*包含拒绝效果的 SCP.将 SCP 附加到组织根

1. 使用 us-west-2 和 eu-central-在 aws 请求区域条件键上使用 StringNotEquals 条件创建一个包含Cloudfront:\*,iam:\*,route53:\*和 support:\*的拒绝效果的 IAM 权限边界 1 个值.将权限边界附加到包含开发和生产用户的 IAM 组
2. 为 AWS 中的组织中的每个开发工作负载创建帐户将开发帐户放置在组织单位(OU)中.创建自定义 Aws Config 规则,以在帐户的每月账单超过 500 美元时停用所有 IAM 用户
3. 在 AWS Organizations 中为组织内的每个开发工作负载创建帐户.将开发帐户放置在组织单位(OU)中. 在 Aws 预算中为每个开发帐户创建预算,以监控并报告每月支出超过 500 美元的情况

答:BCF

Question 213

一家金融公司正在使用在 Amazon EC2 实例上运行的高性能计算集群来进行市场模拟.实例启动时,必须在 Amazon Route 53 私有托管区域中创建DNS 记录.实例终止后,必须删除 DNS 记录.目前,该公司结合使用 Amazon CtoudWatch Events 和 AWS Lambda 来创建 DNS 记录.该解决方案在使用小型群集进行测试时效果很好,但是在包含数千个实例的群集的生产中,该公司在 Lambda 日志中看到以下错误:

-HTTP 400 错误(错误请求).

-响应标头还包括一个值为" Throttling"的状态代码元素和一个值为" Rate beyond"的状态消息元素.

解决方案架构师应该采取哪些步骤来解决这些问题? (选择三个)

答:配置 Amazon SQS FIFO 队列,并配置Cloudwatch Events 规则以将该队列用作目标.从 Cloudwatch Events 规则中删除 Lambda 目标.

1. 配置 Amazon Kinesis 数据流并配置 Cloudwatch Events 规则以将该队列用作目标从Cloudwatch Events 规则中删除 Lambda 目标.
2. 更新 Cloudwatch Events 规则,以触发 Amazon EC2 集群使用的 Auto Scaling 组的"实例启动成功"和" 实例终止成功"事件.
3. 配置 Lambda 函数以从 Amazon SQS 队列中检索消息.修改 Lambda 函数以最多检索 10 条消息,然后按 Amazon Route 53 API 调用类型批处理消息并提交.成功调用 API 后,请从 SQS 队列中删除消息.
4. 配置一个 Amazon SQS 标准队列,并配置现有的 Cloudwatch Events 规则以将该队列用作目标.从

Cloudwatch Events 规则中删除 Lambda 目标.

1. 配置 Lambda 函数以从 Amazon Kinesis 数据流中读取数据,并将批处理窗口配置为 5 分钟.修改该函数, 以使用从 Kinesis 数据读取的所有记录对 Amazon 路线 53 进行单个 API 调用.

答:ACD

Question 214

一家公司使用 Amazon S3 托管 Web 应用程序.当前,该公司使用在 Amazon EC2 实例上运行的持续集成工具,该实例通过将应用程序上载到 S3 存储桶来构建和部署应用程序.

解决方案架构师需要满足以下要求,以增强公司平台的安全性:

-构建过程应在与托管 Web 应用程序的帐户不同的帐户中运行.

-构建过程应在其所使用的帐户中具有最小的访问权限

-不应使用长期使用的凭证首先,开发团队创建了两个 AWS 账户.一个用于名为 Web account 的应用程序. 一个用于构建过程,名为 build account.

解决方案架构师应使用哪种解决方案来满足安全性要求?

答:在构建帐户中,创建一个新的IAM 角色,Amazon EC2 可以假定只有该角色将角色附加到运行持续集成过程的 EC2 实例.创建一个 IAM 策略以允许 s3:在 Web 帐户的 S3 存储桶上调用 putobject.在 Web 帐户中,创建附加到 S3 存储桶的 S3 存储桶策略,该策略允许构建帐户使用 s3:PutObject 调用.

1. 在构建帐户中,创建一个新的IAM 角色,Amazon EC2 只能承担此角色.将角色附加到运行连续集成过程的 EC2 实例.创建一个 IAM 策略以允许 s3:在常规 Web 帐户的 S3 存储桶上调用 Putobject.在 Web 帐户中,创建附加到 S3 存储桶的 S3 存储桶策略,该策略允许新创建的 IAM 角色使用 s3:Putobject 调用
2. 在构建帐户中,创建一个新的 IAM 用户将访问密钥和秘密访问密钥存储在 AWS Secrets Manager 中. 修改连续集成过程,以从 Secrets Manager 中查找 IAM 用户凭据.创建一个 IAM 策略,以允许s3:Putobject 对 Web 帐户中的 S3 存储桶进行校准,并将其附加到用户.在 Web 帐户中,创建附加到 S3 存储桶的 S3 存储桶策略,该策略允许新创建的 IAM 用户使用 s3:Putobject 调用
3. 在构建账户中,修改持续集成过程以从 AWS Secrets Manager 执行 IAM 用户凭证的查找.在 Web 帐户中,创建一个新的 IAM 用户.将访问密钥和秘密访问密钥存储在 Secrets Manager 中.将PowerUserAccess IAM 策略附加到 IAM 用户

答:B

Question 215

一家公司希望通过日期范围和在 AWS 上运行的自定义应用程序来分析日志数据.该应用程序每天产生大约 10 GB 的数据,并且有望增长.

解决方案架构师的任务是将数据存储在 Amazon S3 中,并使用 Amazon Athena 分析数据. 哪个步骤组合将确保随着数据增长而获得最佳性能?(选择两个)

1. 将每个对象存储在 Amazon S3 中,每个键的前面都有一个随机字符串
2. 将数据存储在多个 S3 存储桶中
3. 将数据以列格式(例如 Apache Parquet 或 Apache ORC)存储在 Amazon S3 中. D.将数据存储在小于 10 MB 的对象中的 Amazon S3 中

E.使用包含日期的键在 Amazon S3 中使用 Apache Hive 分区存储数据,例如 dt = 2019-02

答:AC

Question 216

一家公司正在重构现有的 Web 服务,该服务提供对结构化数据的读写访问.该服务必须响应系统负载中短暂但明显的峰值.该服务必须跨多个 AWS 区域容错.

应该采取哪些行动来满足这些要求?

1. 将数据存储在 Amazon DocumentDB 中创建一个单一的全局 Amazon CloudFront 分布,其基于边缘优化的 Amazon API Gateway 和 AWS Lambda 构建自定义来源,将公司域指定为该分布的备用域.并使用CloudFront 分配的别名配置 Amazon Route 53.
2. 将数据存储在两个区域中的已复制 Amazon S3 存储桶中在每个区域中创建一个 Amazon CloudFront 分布,并在每个区域中启动基于 Amazon API Gateway 和 AWS Lambda 的自定义来源,将公司的域分配为两个域的替代域并进行配置 Amazon Route 53 之间具有故障转移路由策略.
3. 使用按需容量模式将数据存储在两个区域中的 Amazon DynamoDB 全局表中在两个区域中,将 Web 服务作为 Amazon ECS Fargate 任务在Amazon Route 中的 Application Load Balancer(ALB)后面的 Auto Scaling ECS 服务中运行 53,在公司域中配置别名记录和基于 Route 53 的基于延迟的路由策略以及运行状况检查,以在两个 ALB 之间分配流量
4. 将数据存储在Amazon Aurora全局数据库。增加AutoScaling Replicas to both regions....

答:~~A~~  最新答案 D

Question 217

移动游戏应用程序将数据连续发布到 Amazon Kinesis Data Streams.

一个 AWS Lambda 函数处理数据流中的记录,并将其写入 Amazon DynamoDB 表. DynamoDB 表启用了自动缩放策略,并将目标利用率设置为 70%.

在每天开始和结束的几分钟内,流量峰值通常超过正常负载的五倍.

该公司注意到,Kinesis 数据流的 GetRecords.IteratorAgeMilliseconds 指标在几分钟内暂时增加到一分钟以上.

在这段时间内,AWS Lambda 函数将预配置的吞吐量超出异常消息写入 Amazon CloudWatch Logs,并且某些记录将重定向到死信队列.

Kinesis 生产商在游戏应用程序上不会引发任何异常. 公司应该做出什么改变来解决这个问题?

1. 使用"应用程序自动扩展"来设置扩展时间表,以扩展服务器上的写容量DynamoDB 表在可预测的负载峰值期间.
2. 使用 Amazon CloudWatch Events 监视死信队列并调用 Lambda 函数自动重试失败的记录.
3. 将 DynamoDB 表自动扩展策略的目标利用率降低到 20%,以更快地响应加载峰值.
4. 增加 Kinesis 数据流中分片的数量以增加吞吐量. 答案:D

Question 218 **03/09考试原题**

一家公司有一个 AWS 主计费账户,这是 AWS Organizations 层次结构的根.该公司在此层次结构中有多个 AWS 账户,所有账户均组织为组织单位(OU).随着业务的其他部分将应用程序迁移到 AWS,将继续创建更多 OUS 和 AWS 帐户.这些业务部门可能需要使用不同的 AWS 服务.安全团队正在为当前和当前所有需求实施以下要求

未来的 AWS 账户.

-必须对所有帐户应用控制策略,以禁止使用 AWS 服务器.

-根据有效的用例,允许控制策略例外.

哪种解决方案将以最少的可选开销满足这些要求?

1. 在组织中使用 SCP 来实施 AWS 服务器的拒绝列表.在等级上应用此 SCP.对于某个 OU 的任何特定例外,请为该 OU 创建一个新 SCP,然后将所需的 AWS 服务添加到允许列表.
2. 使用 SCP In 组织来实施 AWS 服务的拒绝列表.在根级别和每个 OU 上应用此 SCP.从根级别和所有OU 级别删除默认的 AWS 托管 SCP.

对于任何特定的例外,请修改附加到该 OU 的 SCP,然后将所需的 AWS 必需服务添加到允许列表.

1. 在组织中使用 SCP 实施 AWS 服务的拒绝列表.在每个 OU 级别应用此 SCP.将默认的 AWS 受管 SCP

留在根级别.对于某个 OU 的任何特定执行,请为该 OU 创建一个新的 SCP.

1. 在组织中使用 SCP 来实施 AWS 服务的允许列表.在根级别应用此 SCP.从根级别和所有 OU 级别删除默认的 AWS 托管 SCP.

对于某个 OU 的任何特定例外,请修改该 OU 附带的 SCP,然后将所需的AWS 服务添加到允许列表. 答案:B

Question 219

一家零售公司有一个运行在 AWS 上的自定义 NET Web 应用程序,该应用程序使用 Microsoft SQL Server 作为数据库.应用程序服务器在本地维护用户的会话.

需要哪种架构更改组合才能确保解决方案的所有层都高度可用? (选择三个.)

1. 重构应用程序以在 Amazon ElastiCache 中存储用户的会话使用应用程序负载平衡器在应用程序实例之间分配负载
2. 设置数据库以使用 Amazon EBS 每小时生成一次快照配置 Amazon CloudWatch Events 规则以在主数据库实例失败时启动新数据库实例
3. 将数据库迁移到 Amazon RDS tor SQL Server 将 RDS 实例配置为使用 MultiAZ 部署
4. 将 NET 内容移动到 Amazon S3 存储桶为静态网站托管配置存储桶
5. 将应用程序实例放入 Auto Scaling 组中配置 Auto Scaling 组以在实例不正常时创建新实例
6. 在应用程序层之前部署 Amazon CloudFront 配置 CloudFront 以仅提供来自正常应用程序实例的内容答:ACE

Question 220 **11/19考试原题**

一家零售公司在其数据中心的应用程序服务器上处理状态点数据,并将输出写入 Amazon DynamoDB 表. 数据中心通过 AWS Direct Connect(DX)连接连接到公司的 VPC,并且应用程序服务器需要速度超过 2 Gbps 的一致网络连接.

该公司决定 DynamoDB 表需要高度可用且具有容错能力. 公司政策规定,该数据应可在两个地区使用.

公司应进行哪些更改以满足这些要求?

1. 建立第二个 DX 连接以实现冗余.使用 DynamoDB 全局表将数据复制到第二个 Region,修改应用程序以故障转移到第二个 Region.
2. 使用 AWS 托管 VPN 作为 DX 的备份.在第二个区域中创建相同的 DynamoDB 表.修改应用程序以将数据复制到两个区域.
3. 建立第二个 DX 连接以实现冗余.在第二个区域中创建相同的 DynamoDB 表.启用 DynamoDB 自动缩放以管理吞吐量.修改应用程序以写入第二个 Region.
4. 使用 AWS 托管 VPN 作为 DX 的备份.在第二个区域中创建相同的 DynamoDB 表.启用 DynamoDB 流以捕获对表的更改.使用 AWS Lambda 将更改复制到第二个区域.

答 :A Question 221

一家国际公司已在单个区域中部署了依赖 DynamoDB 的多层 Web 应用程序.由于法规方面的原因,他们需要在单独区域中进行灾难恢复

恢复时间目标为 2 小时,恢复点目标为 24 小时.他们应该定期同步其数据,并能够使用 CloudFormation 快速配置 Web 应用程序.目的是最大程度地减少对现有 Web 应用程序的更改,控制用于数据同步的DynamoDB 的吞吐量,并仅同步修改后的元素.

您会选择哪种设计来满足这些要求?

1. 使用 AWS Data Pipeline 每天安排一次 DynamoDB 跨区域副本,在 DynamoDB 表中创建一个" LastUpdated"属性,该属性代表最近一次更新的时间戳并将其用作过滤器
2. 使用 AWS Data Pipeline 安排每天一次将 DynamoDB 表导出到当前区域中的 S3,然后安排另一个任务,

紧接着该任务将数据从 S3 导入另一个区域中的 DynamoDB

1. 使用 EMR 并编写自定义脚本以使用 SCAN 操作从当前区域中的DynamoDB 检索数据,并将其推送到第二个区域中的 DynamoDB
2. 将每个写入也发送到第二个区域中的 SQS 队列中,使用 SQS 队列后面的自动伸缩组在第二个区域中重播写入

答 :A Question 222

您的公司当前在本地数据中心中运行一个 2 层 Web 应用程序.在过去的几个月中,您经历了几次基础架构故障,从而导致重大的财务损失.您的 CIO 强烈考虑将应用程序迁移到 AWS.在努力争取其他公司高管的支持时,他要求您制定灾难恢复计划,以帮助短期内提高业务连续性.他指定了目标

恢复时间目标(RTO)为 4 小时,恢复点目标(RPO)为 1 小时或更短.他还要求您在 2 周内实施该解决方案. 您的数据库大小为 200GB,并且具有 20Mbps 的 Internet 连接.

在最小化成本的同时,您将如何做?

答:创建一个 EBS 支持的私有 AMI,其中包括应用程序的全新安装.开发一个 CloudFormation 模板,其中包括您的 AMI 和所需的 EC2,AutoScaling 和 ELB 资源,以支持跨多个可用性区域部署应用程序.

通过安全 VPN 连接将事务从本地数据库异步复制到 AWS 中的数据库实例.

1. 在多个可用区域中的 Auto Scaling 组内的 EC2 实例上部署应用程序.通过安全 VPN 连接将事务从本地数据库异步复制到 AWS 中的数据库实例.
2. 创建一个由 EBS 支持的私有 AMI,其中包括应用程序的全新安装.在数据中心中设置脚本,以每 1 小时备份一次本地数据库,并使用分段上传功能将生成的文件加密并复制到 S3 存储桶中.
3. 将您的应用程序安装在能够支持应用程序平均负载的,经过计算优化的 EC2 实例上. 通过安全的 Direct Connect 连接将事务从本地数据库同步复制到 AWS 中的数据库实例.

答:A

Question 223

在对服务团队的应用程序进行安全审核期间,解决方案架构师发现可以在 AWS Lambda 功能代码中查看Amazon RDS 数据库的用户名和密码以及一组 AWS IAM 用户凭证. Lambda 函数使用用户名和密码在数据库上运行查询,并且使用 IAM 凭据在单独的管理帐户中调用 AWS 服务.

解决方案架构师担心,凭据可能会将不适当的访问权限授予可以查看 Lambda 代码的任何人.管理帐户和服务团队的帐户位于单独的 AWS Organizations 组织单位(OU)中.

解决方案架构师应进行哪些更改组合以提高解决方案的安全性? (选择两个.) A.将 Lambda 配置为在管理帐户中具有对 AWS 的适当访问权的角色.

1. 将 Lambda 配置为使用 AWS Secrets Manager 中存储的数据库凭证并启用自动轮换.
2. 创建一个 Lambda 函数,通过部署具有更新凭据的新Lambda 版本,每小时轮换凭据.
3. 在管理帐户的 OU 上使用 SCP,以防止 IAM 用户访问服务团队帐户中的资源.
4. 在管理帐户上启用 AWS Shield Advanced,以保护敏感资源免受未经授权的 IAM 访问. 答:~~AB~~ 最新答案：BD

Question 224

您的公司经营着一个面向客户的活动注册网站.该站点以 3 层体系结构构建,具有 Web 和应用层服务器以及 MySQL 数据库.该应用程序需要 6 个 Web 层服务器和 6 个应用程序层服务器才能正常运行,但可以在至少 65%的服务器容量和单个 MySQL 数据库上运行.

在具有三个可用区(AZ)的区域中部署此应用程序时,哪种架构可提供高可用性?

1. 跨 2 个可用区部署的 Web 层,并在 ELB(弹性负载均衡器)后面的Auto Scaling 组内的每个 A2 中具有 3 个 EC2(弹性计算云)实例,并且应用程序层跨 2 个可用区部署,每个 AZ 中具有 3 个 EC2 实例在 ELB 后面的 Auto Scaling 组中,一个 RDS(关系数据库服务)实例与另一个 AZ 中的只读副本一起部署.
2. 跨 3 个 AZ 部署的Web 层,在 ELB(弹性负载均衡器)后面的 Auto Scaling 组内的每个 AZ 中具有 2 个EC2(弹性计算云)实例,并且在 3 个 AZ 中部署的应用层,每个 AZ 中具有 2 个 EC2 实例在 ELB 后面的Auto Scaling 组内部,以及 Multi-AZ RDS(关系数据库服务)部署.
3. 跨两个 AZ 部署的 Web 层,在 ELB(弹性负载均衡器)后面的 Auto Scaling 组内的每个 AZ 中具有 3 个EC2(弹性计算云)实例,并且在两个 AZ 中部署的应用层,每个 AZ 中具有 3 个 EC2 实例 ELB 后面的 Auto Scaling 组内部以及多可用区RDS(关系数据库服务)部署
4. 跨 3 个 AZ 部署的 Web 层,在 ELB(弹性负载平衡器)后面的 Auto Scaling 组内的每个 AZ 中具有 2 个EC2(弹性计算云)实例,并且在 3 个 AZ 中部署的应用层,每个 AZ 中具有 2 个 EC2 实例在 ELB 后面的Auto Scaling 组内部,以及一个 RDS(关系数据库服务)实例,该实例在其他两个 AZ 中部署了只读副本.

答案:B 说明:

<http://highscalability.com/blog/2016/1/11/a-beginners-guide-to-scaling-to-11-million-users-> onamazons.html

https://[www.airpair.com/aws/posts/building-a-scalable-web-app-on-amazon-web-services-p1](http://www.airpair.com/aws/posts/building-a-scalable-web-app-on-amazon-web-services-p1)

Question 225 **03/09考试原题**

管理员正在使用 Amazon CloudFormation 部署由 Web 层和应用程序层组成的三层Web 应用程序,它将利用 Amazon DynamoDB 进行存储.

创建 CloudFormation 模板时,以下哪项将允许应用程序实例访问DynamoDB 表而无需暴露 API 凭据?

1. 创建一个具有所需权限的身份和访问管理角色,以从.required DynamoDB 表中进行读写,并通过引用实例配置文件将该角色与应用程序实例相关联.
2. 创建一个身份和访问管理角色,该角色具有所需的权限,可以从所需的DynamoDB 表中进行读写,并在应用程序实例的实例配置文件属性中引用该角色.
3. 使用 CloudFormation 模板中的 Parameter 部分,让用户从已经创建的 IAM 用户输入访问密钥和秘密密钥,该用户具有从所需 DynamoDB 表进行读取和写入所需的权限.
4. 在 CloudFormation 模板中创建一个身份和访问管理用户,该用户具有从所需 DynamoDB 表中读取和写入的权限,使用 GetAtt 函数检索访问和秘密密钥,并将它们通过用户数据传递给应用程序实例.

答 案 :B Question 226

一个 AWS 客户正在部署一个由 AutoScaling EC2 实例组组成的应用程序.

客户安全策略要求从这些实例到客户虚拟私有云中任何其他服务的每个出站连接都必须使用 包含特定实例 ID 的唯一 X.509 证书.

此外,所有 X.509 证书都必须由客户的密钥管理服务签名,以便可信进行身份验证. 以下哪些配置将支持这些要求?

1. 配置 IAM 角色以授予对包含已签名证书的 Amazon S3 对象的访问权限,并将 Auto Scaling 组配置为使用该角色启动实例.

让实例引导程序在首次启动时从 Amazon S3 获得证书.

1. 配置 Auto Scaling 组将新实例启动的 SNS 通知发送到可信密钥管理服务.让密钥管理服务生成一个签名证书,并将其直接发送到新启动的实例.
2. 将证书嵌入到 Auto Scaling 组使用的 Amazon Machine Image 中.让启动的实例生成具有实例分配给密钥管理服务的实例 ID 的证书签名请求,以进行签名.
3. 配置启动的实例以在首次启动时生成新证书.让密钥管理服务轮询AutoScaling 组中的关联实例并发送新实例

包含特定实例 ID 的证书签名.

答案:B 说明:

该证书必须由客户密钥管理服务签名,这是唯一的选择.使用 S3 不会使其具有唯一性,而将其嵌入 AMI 不会使其具有唯一性,仅凭自身生成新证书将无法满足要求由客户密钥管理服务对其进行签名的要求.

A –从 S3 访问很好,但是每次自动缩放生成不同的实例和实例 ID 时文件如何唯一.那是不可预测的

C –在 AMI 中嵌入证书无法使证书唯一.

D –由于 EC2 实例必须生成唯一的 X.509 证书,并且该证书必须特定于实例 ID. EC2 实例可以自己生成证书,但要明确指出,证书必须由客户密钥管理服务签名,而不是自签名.

Question 227

一家公司拥有一个可在一系列 Amazon EC2 实例上运行的应用程序,并在 Amazon S3 中为每个实例存储

70 GB 的设备数据.最近,一些 S3 上传失败了.

同时,该公司发现存储数据成本意外增加.应用程序代码无法修改.

在管理存储成本的同时将设备数据上传到 Amazon S3 的最有效的方法是什么?

1. 使用分段上传来上传设备数据.使用 AWS CLI 列出不完整的零件以解决失败的 S3 上传.对 S3 存储桶中不完整的分段上传启用生命周期策略,以删除旧的上传并防止新的失败上传累积.
2. 使用 S3 传输加速上传设备数据.使用 AWS 管理控制台解决失败的 S3 上传.每晚使用"多对象删除"操作删除旧的上传文件.
3. 使用分段上传上传设备数据.使用 AWS 管理控制台列出不完整的零件,以解决失败的 S3 上传.配置生命周期策略以连续归档到 Amazon S3 Glacier.
4. 使用 S3 传输加速上传设备数据.使用 AWS 管理控制台列出不完整的零件,以解决失败的S3 上传.对

S3 存储桶中不完整的分段上传启用生命周期策略,以删除旧的上传并防止新的失败上传累积. 答案:A

Question 228 **11/19考试原题**

一家公司正在实施 AWS 组织,以限制其开发人员仅使用 Amazon EC2,Amazon S3 和 Amazon DynamoDB.开发者帐户位于专用的组织单位(OU)中.解决方案架构师已在开发人员帐户中实现了以下SCP:



部署此策略后,Developers 帐户中的 IAM 用户仍可以使用该策略中未列出的 AWS 服务. 解决方案架构师应采取什么措施来消除开发人员使用此政策范围之外的服务的能力?

1. 为应约束的每个 AWS 服务创建一个明确的拒绝语句.
2. 从开发者帐户的 OU 中删除 FullAWSAccess SCP.
3. 修改 FullAWSAccess SCP 以明确拒绝所有服务.
4. 在 SCP 末尾添加一个使用通配符的明确拒绝语句. 答案:B

Question 229

您的公司以前在本地数据中心和 AWS 之间配置了一个使用频繁且动态路由的 VPN 连接.

您最近设置了 DirectConnect 连接,并希望开始使用此新连接.在 AWS 控制台中配置 DirectConnect 设置后,以下哪个选项将为您的用户提供最无缝的过渡?

1. 配置您的 DirectConnect 路由器,更新您的 VPC 路由表以指向 DirectConnect 连接,为您的 VPN 连接配置更高的 BGP 优先级,并验证网络流量是否正确.

利用 DirectConnect 连接.

1. 删除现有的 VPN 连接以避免路由环路,使用适当的设置配置 DirectConnect 路由器,并验证网络流量是否在利用 DirectConnect.
2. 更新您的 VPC 路由表以指向 DirectConnect 连接,使用适当的设置配置 DirectConnect 路由器,确认网络流量正在利用 DirectConnect,然后删除 VPN 连接.
3. 使用比 VPN 路由器更高的 BGP 优先级配置 DirectConnect 路由器,确认网络流量正在利用

DirectConnect,然后删除现有的 VPN 连接.

答案:C 说明:

Direct Connect 优先于动态配置的 VPN 连接.

Question 230

您的团队有一个基于 tomcat 的 Java 应用程序,您需要将其部署到开发,测试和生产环境中.经过研究后,由于其与开发人员工具的紧密集成以及 RDS 的易于管理性,您选择使用 Elastic Beanstalk.您的质量检查小组负责人指出,您需要每晚将一组经过清理的生产数据发布到您的环境中.同样,组织中的其他软件团队也希望通过其 VPC 中的 EC2 实例访问相同的还原数据.满足以上要求的持久性和安全性的最佳设置如下:

答:分别创建您的 RDS 实例,并将其 IP 地址添加到代码中应用程序的 DB 连接字符串中. 更改其安全组,以允许您的 VPC IP 地址块中的主机对其进行访问.

1. 分别创建您的 RDS 实例,并将其 DNS 名称作为环境变量传递给您的 DB 连接字符串. 更改其安全组,以允许您从应用程序子网中的主机对其进行访问.
2. 创建您的 RDS 实例作为 Elastic Beanstalk 定义的一部分,并更改其安全组,以允许您从应用程序子网中的主机对其进行访问.
3. 单独创建 RDS 实例,并将其 DNS 名称作为环境变量传递到应用程序的 DB 连接字符串.

为客户端计算机创建一个安全组,并将其作为数据库流量的有效源添加到 RDS 实例本身的安全组.

答案:D 说明:

Elastic Beanstalk 提供了在 Elastic Beanstalk 环境中运行 Amazon RDS 实例的支持.这对于开发和测试环境非常有效,但对于生产环境而言并不理想,因为它将数据库实例的生命周期与应用程序环境的生命周期联系在一起.

<http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.RDS.html>

Question 231

您有一个定期的图像分析应用程序,该应用程序在输入中获取一些文件,对其进行分析,然后为每个文件将 输出中的一些数据写入文本文件.每天输入的文件数量很多,并且集中在一天的几个小时内.

当前,您在 EC2 上有一台具有大 EBS 卷的服务器,用于承载输入数据和结果.每天大约需要 20 个小时才能完成该过程.

可以使用哪些服务来减少设计时间并提高解决方案的可用性?

1. S3 用于存储 I / O 文件,SQS 用于将详细说明命令分发给并行工作的主机组,Auto Scaling 可根据 SQS

队列的长度动态调整主机组的大小.

1. S3 用于存储 I / O 文件,SNS 用于将详细说明命令分发给并行工作的主机组,Auto Scaling 可根据 SNS

通知的数量动态调整主机组的大小.

1. 具有预配置 IOPS(PIOPS)的 EBS,用于存储 I / O 文件； SNS,用于将精化命令分发给并行工作的主机组； Auto Scaling,可动态调整主机组的大小

取决于 SNS 通知的数量.

1. 具有预配置 IOPS(PIOPS)的 EBS 用于存储 I / O 文件,SQS 用于将详细说明命令分发给一组并行工作的主机. Auto Scaling 可动态调整主机组的大小

取决于 SQS 队列的长度.

答:A

说明:

SNS 不允许您在主机组之间分配任务.它允许您发送通知,但是您如何确定将由哪个主机处理呢? 同样,PIOPS 有利于性能,但不适用于此任务要求的可用性.

使用 S3 没问题,因为没有频繁更改的数据,您只需处理文件并写入一次结果,以后就不要更改.

Question 232

由于 Amazon S3 存储桶上的权限问题,一家公司经历了高度机密的个人信息泄露.信息安全团队已加强了存储桶策略以限制访问.此外,为了更好地为将来的攻击做准备,必须满足以下要求:

-识别正在访问存储桶对象的远程 IP 地址.

-更改存储桶上的安全策略时接收警报.

-自动修复策略更改.

解决方案架构师应使用哪些策略?

1. 将 Amazon CloudWatch Logs 与 CloudWatch 过滤器一起使用以标识远程 IP 地址.将 CloudWatch Events 规则与 AWS Lambda 结合使用可自动修复 S3 存储桶策略更改.结合使用 Amazon SES 和CloudWatch Events 规则来警报.
2. 将 Amazon Athena 与 S3 访问日志一起使用以标识远程 IP 地址.结合使用 AWS Config 规则和 AWS Systems Manager Automation,可以自动修复 S3 存储桶策略更改.结合使用 Amazon SNS 和 AWS Config 规则来警报.
3. 将 S3 访问日志与 Amazon Elasticsearch Service 和 Kibana 一起使用以标识远程 IP 地址.使用

Amazon Inspector 评估模板自动补救 S3 存储桶策略更改.使用 Amazon SNS 发出警报.

1. 将 Amazon Macie 与 S3 存储桶一起使用,以识别访问模式和远程 IP 地址.将 AWS Lambda 与 Macie

结合使用可自动修复 S3 存储桶策略更改.使用 Macie 自动警报功能进行警报. 答:B

Question 233

一个组织计划在通过 VPC 启动的单个实例上托管 Wordpress 博客和 joomla CMS.组织希望为每个应用程序使用单独的域,并使用Route 53 进行分配.组织可能有大约十个实例,每个实例都有两个应用程序,如上所述.在启动实例时,组织配置了两个单独的网络接口(主要+ ENI),并希望为该实例具有两个弹性 IP.

由于弹性 IP 的数量受到限制,建议使用 AWS 的公共 IP 代替弹性 IP.

您会建议该组织采取什么行动?

答:我同意该建议,但希望组织将每个 ENI 使用单独的子网用于不同的公共 IP.

1. 我不同意,因为一个实例具有多个 ENI,并且 AWS 不会将公共 IP 分配给具有多个 ENI 的实例,所以只需要具有弹性 IP.
2. 我不同意,因为 AWS VPC 不会将公共 IP 附加到ENI；因此用户仅需使用弹性 IP. D.我同意该建议,建议使用 AWS 的公共 IP,因为该组织将使用 DNS 与 Route 53.

答案:B 说明:

虚拟私有云(VPC)是专用于用户的 AWS 账户的虚拟网络.它使用户可以将 AWS 资源启动到用户已定义的虚拟网络中.弹性网络接口(ENI)是一个虚拟网络接口,用户可以将其附加到 VPC 中的实例.用户可以在一个实例中最多附加两个 ENI.但是,当有两个 ENI 附加到单个实例时,AWS 无法分配公共 IP.建议在这种情 况 下 分 配 弹 性 IP. 如 果 组 织 想 要 超 过 5 个 EIP, 则 可 以 请 求 AWS 增 加 数 量 .<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>

Question 234

解决方案架构师希望确保只有 AWS 用户或具有适当权限的角色才能访问新的 Amazon API Gateway 终端节点.解决方案架构师希望获得每个请求的端到端视图,以分析请求的延迟并创建服务映射.

Solutions Architect 如何设计 API 网关访问控制并执行请求检查?

1. 对于 API Gateway 方法,将授权设置为 AWS\_IAM.然后,向 IAM 用户或角色执行 REST API 资源上的execute-api:Invoke 权限.访问终端节点时,使 API 调用程序可以使用 AWS Signature 签名请求.使用AWS X-Ray 跟踪和分析对 API Gateway 的用户请求.
2. 对于 API 网关资源,将 CORS 设置为 enabled,并且仅在 Access-Control-Allow-Origin 标头中返回公司的域.然后,向 IAM 用户或角色执行 REST API 资源上的 execute-api:Invoke 权限.使用 Amazon CloudWatch 跟踪和分析对 API 网关的用户请求.
3. 创建一个 AWS Lambda 函数作为自定义授权者,要求 API 客户端在进行调用时传递密钥和机密,然后使用 Lambda 针对 IAM 系统验证密钥/秘密对.

使用 AWS X-Ray 跟踪和分析对 API Gateway 的用户请求.

1. 为 API 网关创建客户端证书.将证书分配给需要访问终端节点的 AWS 用户和角色.访问端点时,使 API

调用程序能够通过客户端证书.使用 Amazon CloudWatch 跟踪和分析对 API 网关的用户请求. 答案:A

Question 235

一家公司每小时在其主要的事务数据库上运行批处理分析.在 RDS MySQL 实例上运行以填充在

Redshift 上运行的中央数据仓库.在批处理执行期间,其事务应用程序非常慢.

批处理完成后,他们需要使用新数据更新顶级管理仪表板.该仪表板是由本地运行的另一个系统生成的,当 手动发送的电子邮件通知您需要更新时,该系统当前已启动.已修改,因为是由另一个团队管理的.

您如何优化此方案以解决性能问题并尽可能使流程自动化?

1. 用 Redshift 替换 RDS 以进行批处理分析和 SNS,以通知本地系统更新仪表板
2. 将 ROS 替换为Redsnift 以进行oaten 分析和 SQS,以向内部部署系统发送消息以更新仪表板C.创建用于批处理分析和 SNS 的 RDS 只读副本,以通知我本地系统更新仪表板

D.创建用于批处理分析和 SQS 的 RDS 只读副本,以将消息发送到本地系统以更新仪表板.

答案:C 说明:

如果您想防止报告和分析处理干扰 OLTP 工作负载的性能."

如果我正确理解了以上说法,他们就是说将报告和分析处理与 OLTP 分开.换句话说,使用 RedShift 进行报告和分析处理并使用

用于 OLTP 工作负载的 RDS.

Question 236

一家公司正在为一个受欢迎的电视节目建立投票系统,观众将观看表演,然后访问该节目的网站以投票选 出他们最喜欢的表演者.预计在展会结束后的短时间内,该网站将接待数百万名访客,

访问者将首先使用其 Amazon.com 凭据登录该网站,然后提交投票.

投票完成后,页面将显示投票总数.该公司需要构建该站点,以便它可以处理流量的快速流入,同时保持良好 的性能,而且

希望将成本降到最低.

他们应使用以下哪个设计模式?

1. 在一组自动缩放的 Web 服务器之前使用 CloudFront 和 Elastic Load Balancer,这些 Web 服务器将首先调用 Login With Amazon 服务来对用户进行身份验证,这些 Web 服务器将处理用户的投票并将结果存储到使用 IAM 角色的 EC2 实例的DynamoDB 表来获得对 DynamoDB 表的权限.
2. 在一组自动缩放的 Web 服务器之前使用 CloudFront 和 Elastic Load Balancer,这些 Web 服务器将首先调用 Login With Amazon 服务对用户进行身份验证,这些 Web 服务器将处理用户的投票并将结果存储到使用 EC2 实例的 IAM 角色获取 SQS 队列的权限的 SQS 队列.

然后,一组应用程序服务器将从队列中检索项目,并将结果存储到 DynamoDB 表中.

1. 在一组自动缩放的 Web 服务器之前使用 CloudFront 和 Elastic Load Balancer,这些 Web 服务器将首先调用 Login With Amazon 服务来对用户进行身份验证,然后处理

用户投票并将结果存储到多可用区关系数据库服务实例中.

1. 将 CloudFront 和 S3 的静态网站托管功能与 Javascript SDK 一起使用来调用"使用亚马逊登录"服务以对用户进行身份验证,使用 IAM 角色来获得对

DynamoDB 表存储用户投票. 答案:B

Question 237

软件即服务(SaaS)公司为私有律师事务所和公共部门提供用于文档管理的云解决方案.一位当地政府客户最近要求,高度机密的文档不能在国外存储.公司的CIO 要求解决方案架构师确保应用程序可以适应这一新要求. CIO 还希望为这些文档制定适当的备份计划,因为当前未执行备份.

哪种解决方案可以满足这些要求?

1. 在 Amazon S3 中标记不高度机密的文档. 为每个用户创建单独的 S3 存储桶.

将对象上传到每个用户的存储桶.

将 S3 存储桶复制从这些存储桶设置到另一个 AWS 账户和 AWS 区域中的中央 S3 存储桶.

配置由 Amazon CloudWatch 中的计划事件触发的AWS Lambda 函数,以删除在 S3 备份存储桶中标记为秘密的对象.

1. 在 Amazon S3 中将文档标记为常规或秘密.

在相同的 AWS 账户和 AWS 区域中创建一个单独的 S3 备份存储桶. 在单独的 AWS 账户中创建跨区域 S3 存储桶.

设置适当的 IAM 角色以允许对 S3 存储桶进行跨区域许可.

配置由 Amazon CloudWatch 计划的事件触发的 AWS Lambda 函数,将标记为秘密的对象复制到S3 备份存储桶以及标记为跨区域 S3 存储桶的对象.

1. 在 Amazon S3 中将文档标记为常规文档或秘密文档.

在相同的 AWS 账户和 AWS 区域中创建一个单独的 S3 备份存储桶.

使用基于对象标签的 S3 选择性跨区域复制将常规文档移动到其他 AWS 区域中的 S3 存储桶.

配置一个 AWS Lambda 函数,该函数在在主存储桶中创建新的 S3 对象时触发,以仅将标记为密钥的文档复制到同一 AWS 区域中的 S3 存储桶中.

1. 在 Amazon S3 中将高度机密的文档标记为机密.在相同的 AWS 账户和 AWS 区域中创建一个单独的

S3 备份存储桶.

使用基于对象标签的 S3 选择性跨区域复制将常规文档移动到其他 AWS 区域中的 S3 存储桶.

为标记为 secret 的新 S3 对象创建 Amazon CloudWatch Events 规则,以触发 AWS Lambda 函数将其复制到同一 AWS 区域中的单独存储桶中.

答案:D

Question 238

您正在开发新的移动应用程序,并正在考虑在 AWS 中存储用户首选项.这将为使用多个移动设备访问应用程序的用户提供更统一的跨设备体验.每个用户的偏好数据估计为 50KB.此外,预计将有 500 万客户定期使用该应用程序.

该解决方案必须具有成本效益,高可用性,可扩展性和安全性. 您将如何设计满足以上要求的解决方案?

1. 在 2 个可用区中设置具有多个只读副本的 RDS MySQL 实例,以存储用户首选项数据.

移动应用程序将从已读取的副本中查询用户首选项.利用 MySQL 用户管理和访问权限系统来管理安全性和访问凭据.

1. 在 2 个可用区中设置一个 RDS MySQL 实例来存储用户首选项数据.

在数据库前面的服务器上部署面向公众的应用程序,以管理安全性和访问凭据.

1. 将用户偏好数据存储在 S3 中.设置一个 DynamoDB 表,其中包含每个用户的项目以及指向用户 S3 对象的 item 属性.

移动应用程序将从 DynamoDB 检索 S3 URL,然后直接访问 S3 对象.

利用 STS,Web Identity Federation 和 S3 ACL 对访问进行身份验证和授权.

1. 为每个用户设置一个 DynamoDB 表,该表具有一个项目,该项目具有保存用户首选项的必要属性. 移动应用程序将直接从 DynamoDB 表查询用户首选项.

利用 STS,Web Identity Federation 和 DynamoDB 细粒度访问控制对访问进行身份验证和授权. 答案:D

说明:

https://aws.amazon.com/blogs/aws/fine-grained-access-control-for-amazon-dynamodb/

您可以使用细粒度的访问控制来构建以下内容:

一个移动应用程序,根据用户的位置显示附近机场的信息.该应用程序可以访问和显示属性,例如航空公司 名称,到达时间和航班号.然而,

它无法访问或显示飞行员姓名或乘客人数.

在单个表格中为所有用户存储高分的手机游戏.每个用户都可以更新自己的分数,但无法访问其他分数.

Question 239

您想使用 AWS CodeDeploy 将应用程序部署到在 Amazon Virtual Private Cloud(VPC)中运行的Amazon EC2 实例.

必须满足什么条件?

答:安装在 Amazon EC2 实例上的 AWS CodeDeploy 代理必须只能访问公共 AWS CodeDeploy 终端节点.

1. 安装在 Amazon EC2 实例上的 AWS CodeDeploy 代理必须只能访问公共 Amazon S3 服务终端节点.
2. 安装在 Amazon EC2 实例上的 AWS CodeDeploy 代理必须能够访问公共 AWS CodeDeploy 和

Amazon S3 服务终端节点.

1. 当前无法使用 AWS CodeDeploy 将应用程序部署到在 Amazon Virtual Private Cloud(VPC)中运行的Amazon EC2 实例.

答案:C

说明:

您可以使用 AWS CodeDeploy 将应用程序部署到在 Amazon Virtual Private Cloud(VPC)中运行的Amazon EC2 实例.

但是,安装在Amazon EC2 实例上的 AWS CodeDeploy 代理必须能够访问公共 AWS CodeDeploy 和

Amazon S3 服 务 终 端 节 点 .<http://aws.amazon.com/codedeploy/faqs/>

Question 240

在调试支持全球分布式的 IoT 系统的后端应用程序时

解决方案架构师注意到,过时的数据偶尔会发送到用户设备.

设备通常共享数据,并且在大多数情况下,陈旧的数据不会引起问题.但是,设备 设备在更新后读取陈旧数据时,操作会中断.

全局系统在不同的 AWS 区域中部署了多个相同的应用程序堆栈.如果用户设备离开其本国地理区域旅行时,它将始终连接到

地理位置最接近的 AWS 区域以写入或读取数据.相同的数据在所有

Amazon DynamoDB 全局表来支持受支持的 AWS 区域. 应该进行哪些更改以避免引起设备操作中断?

1. 更新后端以使用高度一致的读取.更新设备以始终写入和读取其本地 AWS 区域.
2. 在 DynamoDB 全局表上全局启用强一致性. 更新后端以使用高度一致的读取.
3. 将后端数据存储区切换到具有跨区域副本的 Amazon Aurora MySQL.

更新后端以始终写入主端点.

1. 选择一个 AWS 区域作为主服务器,并仅在该 AWS 区域中执行所有写入. 更新后端以使用高度一致的读取.

答:A

Question 241

一家公司开发了 Java 应用程序并将其部署到在 Amazon EC2 实例上运行的 Apache Tomcat 服务器.该公司的工程团队已实施 AWS CloudFormation 和 Chef Automate,以在开发,测试和生产环境中自动化对应用程序的基础架构和配置的供应和更新.这些实现已大大提高了发布更改的可靠性.工程团队报告,在更 新 Apache Tomcat 服务器的应用程序时,由于意外错误而经常导致服务中断.

哪种解决方案将提高所有版本的可靠性?

A.实施蓝/绿部署方法.

1. 实施金丝雀释放方法.
2. 配置 Amazon CloudFront 以在部署更新时满足来自缓存的所有请求.
3. 一次实施全部部署方法.

答 :A

Question 242 **12/12考试原题** **11/19考试原题 03/09考试原题**

开发人员想要为 AWS Systems Manager 实施多账户访问,并计划在其 AWS 组织内使用两个成员账户. 开发人员已经委派了一个 IAM 角色,该角色允许会员帐户信任 Systems Manager(SSM)参数存储和文档资源.在测试来自会员帐户的访问权限时,用户在执行任何与 SSM 相关的操作时会收到"访问被拒绝"错误. 解决方案架构师确认,在任何组织的服务控制策略(SCP)中都不会拒绝 SSM 操作.两个成员帐户都被移入了一个与任何拒绝 SCP 都不相关的测试 OU,但是用户仍然收到拒绝访问错误.

解决方案架构师应该进行哪些更改以在保持最小特权的同时提供访问权限?

1. 创建一个允许 SSM 操作的新 SCP,并为每个 SSM 参数存储和文档指定 ARNS.将新 SCP 应用于成员帐户所在的测试 OU.
2. 创建一个新的 SCP,该 SCP 允许完全访问 AWS 资源.将新 SCP 应用于成员帐户已移至的测试 OU C.从当前组织中删除两个成员帐户.创建一个新的组织,将拥有 SSM 资源的帐户作为新的主帐户,将另一个帐户作为新组织的成员.创建一个新的SCP,以允许完全访问 AWS 资源

D.从当前组织中删除两个成员帐户.创建一个新的组织,将拥有 SSM 资源的帐户作为新的主帐户,将另一个帐户作为新组织的成员.创建一个允许SSM 操作的新 SCP,并为新主帐户中的每个 SSM 参数存储和文档指定 ARN

答:D

Question 243 **12/12考试原题 03/09考试原题 03/23考题**

一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 组织,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.他们还想将多个帐户作为一个单位一起管理.

解决方案架构师应采取哪些步骤来满足这些要求?(选择三个) A.使用拒绝列表策略

1. 在 AWS IAM 中查看 Access Advisor,以确定
2. 查看 AWS Trusted Advisor 报告以确定最近使用的服务
3. 删除默认的 Fullansaccess Scp
4. 定义组织单位(OUS)并将会员帐户放入 Ous F.删除默认的 Denyawsaccess SCP

答:CDE

Question 244 **11/19考试原题 03/09考试原题**

一家公司使用 Amazon ECS 集群中托管的 Application Load Balancer(ALB)和 Docker 应用程序托管社区论坛站点.站点数据存储在 Amazon RDS for MYSQL 中,而容器映像存储在 ECR 中.公司需要为其客户提供废料回收 SLA,其 RTO 不超过 24 小时,RPO 不超过 8 小时.

以下哪种解决方案是符合要求的最具成本效益的方法?

1. 使用 AWS Cloudformation 在两个区域中部署相同的 ALB,EC2,ECS 和 RDS 资源.每 8 小时安排一次RDS 快照.使用 RDS 多区域复制来更新数据库的辅助区域副本.如果发生故障,请从最新快照还原,然后使用 Amazon Route 53 DNS 故障转移策略将客户自动重定向到辅助区域中的 ALB
2. 将 Docker 映像存储在两个区域的 ECR 中.每 8 小时安排一次 RDS 快照,并将快照复制到辅助区域.如果发生故障,请使用AWS Cloudformation 在辅助区域中部署 ALB,EC2,ECS 和 RDS 资源,从最新快照还原,并更新 DNS 记录以指向辅助区域中的 ALB
3. 使用 AWS Cloudformation 在辅助区域中部署相同的 ALB,EC2 ECS 和 RDS 资源.将每小时的 RDS MYSQL 备份安排到 Amazon S3,并使用跨区域复制将数据复制到辅助区域中的存储桶.发生故障时,将最新的 Docker 映像导入辅助区域中的 Amazon ECR,部署到EC2 实例,还原最新的 MYSQL 备份,并更新DNS 记录以指向辅助区域中的 ALB
4. 在 AWS Auto Scaling 组中使用 ALB 和 Docker 的最小 resourceEC2 部署在辅助区域中部署指示灯环境,并具有扩展策略以增加实例大小和节点数.创建 RDS 数据的跨区域读取副本.如果发生故障,请将副本提升为主服务器,并更新 DNS 记录以指向辅助区域中的 ALB.

答:C

Question 245 **12/12考试原题11/19考试原题 03/09考试原题 03/23考题**

解决方案架构师需要将本地旧版应用程序迁移到 AWS.该应用程序在负载均衡器后面的两台服务器上运行.该应用程序需要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 个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

满足这些要求,应该采取哪些步骤组合才能为 AWS 中的应用程序服务器启用高度可用的体系结构?(选择两个)

1. 创建一个 ENI 池.向供应商请求用于池的许可证文件,并将许可证文件存储在 Amazon S3 中.创建引导程序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.向供应商请求该池的许可证文件,并将许可证文件存储在 Amazon EC2 实例上.从实例创建 AMI,并将此 AMI 用于将来的所有 EC2 实例
3. 创建一个引导程序自动化脚本,以要求供应商提供新的许可证文件.收到响应后,将许可证文件应用于Amazon EC2 实例
4. 编辑引导程序自动化脚本以从 AWS Systems Manager 参数存储读取数据库服务器 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,并重新创建 AMI 以用于将来的所有EC2 实例

答:AD

Question 246 **12/12考试原题** **11/19考试原题 03/09考试原题 03/23考题**

一家公司正在其 Development VPC 中测试 Amazon Elastic File Service(EFS),并希望在本地扩展此测试.EFS 在 us-east-1 中运行,并且公司网络当前已通过站点到该区域的连接站点 VPN.要求所有本地计算机和服务器都处理由其本地 DNS 服务器解析的所有 DNS 流量.本地用户希望使用 UNS 名称而不是 IP 地址连接到 EFS.

为了满足此要求必须采取哪些步骤?(选择两个)

1. 使用域名 awscloud.example.com 创建一个新的 Amazon Route 53 私有托管区域,并将 Development VPC 与此区域关联.创建一个 CNAME 记录,并将其指向 EFS 端点.
2. 使用域名 awscloud.example.com 创建一个新的 Amazon Route 53 公共托管区域,并将 Development VPC 关联到该区域.创建一个 CNAME 记录并将其指向 EFS 端点
3. 在本地 DNS 服务器中创建条件转发器规则,以将对awscloud.example.com 的请求转发到 Amazon Route 53 解析器入站终端节点
4. 在本地 DNS 服务器中创建条件转发器规则,以将对awscloud.example.com 的请求转发到 Amazon Route 53 解析器出站终端节点
5. 在本地 DNS 服务器中创建条件转发器规则,以将对 awscloud.example.com 的请求转发到 Amazon 提供的 DNS 服务器

答:BC

Question 247 **12/12考试原题** **11/19考试原题 03/09考试原题**

一组研究机构正在合作研究 2 PB 定期变化的基因组数据.拥有数据的主要机构正在将其存储在其 AWS 账户的 Amazon S3 存储桶中.合伙企业中的所有二级机构都有自己的 AWS 账户,并要求对数据具有读取权限.拥有数据的机构并不想支付与允许二级机构访问数据相关的数据传输成本.

以下哪个解决方案可以满足要求?

1. 在主要帐户中,为每个辅助帐户创建一个跨帐户 AWS IAM 角色,以允许对数据进行读取访问.让二级机构在访问数据时扮演角色
2. 在主要帐户中,创建一个 S3 存储桶策略以授予对每个次要帐户的读取访问权限.在 S3 存储桶上启用请求者付款.在访问数据时,让二级机构使用自己的 AWS 凭证以及对 S3 存储桶的读取权限
3. 在 S3 存储桶策略中为每个辅助帐户创建一个 S3 存储桶策略,该策略提供对主帐户的写访问权限.定期将 S3 存储桶从主帐户同步到每个辅助帐户.让二级机构在访问数据时使用自己的 AWS 凭证
4. 在主要账户中,为每个辅助账户创建一个跨账户 AWS IAM 角色,该角色允许对数据启用请求者 Payson S3 存储桶的读取访问.让二级机构在访问数据时扮演角色

答:B

Question 248

一家公司计划部署一个新的业务分析应用程序,该应用程序每个月需要 10.000 个小时的计算时间.计算资源可以具有灵活的可用性,但必须满足以下条件:

尽可能节省成本.该公司还将提供报告服务,以分发分析数据 报告,该报告需要始终运行.

解决方案架构师应如何设计满足这些要求的解决方案?

答:在现场 Fleet 上部署报告服务.使用 Aw 部署分析 ECS.当他计算 opon 时再次出现.分析应用程序或通过 Service Auto Scaling 使用自定义指标

1. 在按需实例上部署报告服务以 AWS Fargate 作为计算选项,将分析应用程序部署为 AWS Batch 中的容器.将分析应用程序设置为对 Service Auto Scaling 使用定制指标.
2. 将报告服务部署为 Amazon ECS 中的容器,而将 AWS Fargate 作为计算优化器部署在 Spot Fleet 上. 设置分析应用程序以将自定义指标与适用于 Spot Fleet 的 Amazon EC2 Auto Scaling 一起使用
3. 将报告服务部署为 Amazon ECS 中的容器,并使用 AWS Fargate 作为计算选项.在按需实例上部署分析应用程序,并购买为期三年的储备实例.设置分析应用程序以使用自定义指标,并将 Amazon EC2 Auto Scaling 应用于按需实例

答案:C

**--------------------------------33 New Question ----------------------------**

Question 1

一家公用事业公司希望每 5 分钟从其智能电表收集一次使用数据,以方便使用时计量.当仪表将数据发送到 AWS 时,数据将发送到 Amazon API Gateway,由 AWS Lambda 函数处理,并存储在 Amazon Dynamodb 表中.在试验阶段,Lambda 函数需要 3 到 5 秒钟才能完成.随着更多智能仪表的部署,工程师注意到 Lambda 功能需要 1 到 2 分钟才能完成.随着从设备中收集新类型的指标,功能的持续时间也在增加. 在 Dynamodb 上执行 PUT 操作时,存在许多 ProvisionedThroughputExceedeException 错误,并且来自Lambda 的 TooManRequestsException 错误也很多.

哪种更改组合可以解决这些问题?(选择两个)

A.增加对 Dynamodb 表的写入容量单位

1. 增加 Lambda 函数可用的内存
2. 增加智能电表的有效负载大小以发送更多数据
3. 将数据从 Apl Gateway 传输到 Amazon Kinesis 数据流中,并分批处理数据
4. 在 Amazon SQS FIFO 队列中收集数据,这会触发 Lambda 函数来处理每条消息

答:AD

Question 2

一家公司正在开发一项新服务,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很高的可用性,并且在各个可用区之间都具有冗余性,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,以便其他公司可以添加地址他们的允许清单. 假设在单个区域的多个可用区中部署了资源,哪种解决方案将满足这些要求?

1. 使用每个实例的弹性 IP 地址创建 Amazon EC2 实例.创建一个网络负载平衡器(NLB)并公开静态 TCP

端口.向 EC2 实例注册

NLB.创建一个名为 my.service.com 的新名称服务器记录集,并将 EC2 实例的弹性 IP 地址分配给该记录集.将 EC2 实例的弹性 IP 地址提供给其他公司,以添加到其允许列表中.

1. 为该应用程序创建一个 Amazon ECS 集群和服务定义.为 ECS 集群创建并分配公网IP 地址.创建一个网络负载均衡器(NLB)并暴露 TCP 端口.创建一个目标组并将 ECS 群集名称分配给 NLB.创建一个名为my.service.com 的新 A 记录集,并将 ECS 群集的公共 IP 地址分配给该记录集.将 ECS 群集的公共 IP 地址提供给其他公司以添加到其允许列表中.
2. 为该服务创建 Amazon EC2 实例.为每个可用区创建一个弹性 IP 地址.创建一个网络负载平衡器(NLB) 并公开分配的 TCP 端口.将弹性 IP 地址分配给每个可用区的 NLB.创建一个目标组并向 NLB 注册 EC2 实例.创建一个名为my.service.com 的新 A(alias)记录集,并将 NLB DNS 名称分配给该记录集.
3. 为应用程序创建一个 Amazon ECS 集群和服务定义.为群集中的每个主机创建并分配公共 IP 地址.创建一个应用程序负载平衡器(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 地址与该记录集相关联.将 Amazon EC2 实例的弹性 IP 地址提供给其他公司,以添加到其允许列表中.

答:C

Question 3

一家公司正在运行一个 Web 应用程序,该应用程序具有 Auto Scaling 组中的按需 Amazon EC2 实例,这些实例根据自定义指标进行动态扩展.经过广泛的测试后,该公司确定 m5.2xlarge 实例大小对于工作负载是最佳的.应用程序数据存储在 db r4.4xlarge Amazon RDS 实例中,该实例已确认是最佳实例.到 Web 应用程序的流量在一天中随机增加.

公司还应采用哪些其他成本优化方法来进一步降低成本而又不影响应用程序的可靠性?

1. 将 Auto Scaling 组中的实例计数加倍,并将实例大小减小为 m5.large
2. 为 rds 数据库保留容量和恒定运行的 EC2 实例的最小数量
3. 将 RDS 实例大小减小为 db r4xlarge,并添加五个同等大小的只读副本以提供可靠性
4. 为所有 EC2 实例保留容量,并为 rds 数据库利用竞价型实例定价.

答:C

Question 4 **11/19考试原题**

一家拥有多个账户的公司当前使用的配置不符合以下安全监管政策:防止从端口 22 进入任何 Amazon EC2 实例的入口,需要资源的账单和应用程序标签.加密所有 Amazon EBS 卷.解决方案架构师希望如果存在政策偏差,则提供预防和侦查控制,包括有关特定资源的通知.

解决方案架构师应实施哪种解决方案?

1. 创建一个 AWS Code Commit 存储库,其中包含与策略兼容的 AWS Cloudformation 模板.创建一个

AWS Service Catalog 产品组合.通过将代码提交存储库附加到产品组合来导入 Cloudformation 模板.

将所有帐户中的用户限制为使用 AWS Service Catalog 产品组合中的项目.使用 AWS Config 托管规则来检测与策略的偏差.为偏差配置 Amazon Cloudwatch 事件规则,并在 TriggeredRules 指标大于零时关联Cloudwatch 警报以发送通知.

1. 使用 AWS 服务目录构建包含符合中央账户中的治理策略的产品的产品组合.将所有帐户中的用户限制为使用 Aws Service Catalog 产品.与其他帐户共享合规的投资组合.使用 AWS Config 托管规则来检测与策略的偏差.配置 Amazon Cloudwatch Events 规则以在发生偏差时发送通知
2. 为每个帐户实施符合政策的 AWS Cloudformation 模板,并确保所有供应均由 Cloudformation 完成.配置 Amazon Inspector 以对资源执行常规检查.执行策略验证,并将评估输出写入 Amazon CloudwatchLogs.创建 Cloudwatch Logs 指标过滤器以在出现偏差时增加指标.配置 Cloudwatch 警报以在配置的指标大于零时发送通知
3. 限制用户并使用 AWS IAM 强制执行最小特权访问.将所有 AWS CloudTrail 日志整合到一个账户中.将Cloud Trail 日志发送到 Amazon Elasticsearch Service(Amazon ES).使用 Amazon ES 中的 Kibana 仪表板和 Amazon SNS 实施监视,警报和报告.

答 :B

Question 5

一家公司正在使用其源代码管理器中的 HTTP Webhook 来执行代码漏洞扫描.漏洞扫描由运行在 Aws Lambda 中的应用程序完成,该应用程序在收到 Webhook 时由 Amazon Apl Gateway 调用.源控制平台需要在 30 秒内从 Webhook 目标发出 HTTP 200 响应.否则,将重新发送 Webhook.代码漏洞扫描最多可能需要 10 分钟才能完成,具体取决于要扫描的代码库的大小.该公司希望确保每个Webhook 仅触发一次漏洞扫描.

哪种解决方案可以满足公司的要求?

1. 将 Lambda 函数的 Apl Gateway 集成类型更改为 AWS\_PROXY.在继续执行漏洞扫描之前,修改Lambda 代码以在调用 HTTP 200 响应后立即返回.
2. 创建一个新的 Lambda 函数,由 API Gateway 调用以将 Webhook 写入具有消息重复数据删除功能的Amazon SQS FIFO 队列中,然后返回 HTTP 200 响应从 SQS FIFO 队列中的消息触发代码漏洞扫描程序C.配置 API 网关以异步调用 Lambda 函数.将 Lambda 函数调用后,向 API 网关添加集成响应以返回HTTP 200 响应

D 配置 API 网关以异步调用 Lambda 函数.在继续执行漏洞扫描之前,修改 Lambda 代码以在调用 HTTP 200 响应后立即返回.

答:B

Question 6

一家公司拥有一个复杂的 Web 应用程序,该应用程序利用 Amazon Cloudfront 来实现全球可扩展性和性能.随着时间的流逝,用户报告 Web 应用程序正在变慢.该公司的运营团队报告说 Cloudfront 缓存命中率一直在稳步下降.这些缓存指标报告表明某些 URL 上的查询字符串的顺序不一致,有时以大小写字母混合, 有时以小写字母指定.

解决方案架构师应采取哪些行动来尽可能快地增加缓存命中率?

1. 部署 Lambda @ Edge 函数以按名称对参数进行排序并将其强制为小写选择 Cloudfront 查看器请求触发器以调用该函数
2. 更新 Cloudf ront 发行版以基于查询字符串参数禁用缓存
3. 在负载均衡器之后部署反向代理以对应用程序中发出的 URL 进行后处理以强制 URL 字符串小写
4. 更新 Cloudfront 发行版以指定不区分大小写的查询字符串处理

答:D

Question 7

一家公司在未连接到公司网络的 VPC 的公共子网和私有子网中都有多个 Amazon EC2 实例.与 EC2 实例相关联的安全性组使该公司可以在该 Internet 上使用 Windows 远程桌面协议(RDP)来访问该实例.安全团队注意到来自未知来源的连接尝试.该公司希望实施更安全的解决方案来访问EC2 实例

解决方案架构师应采用哪种策略?

1. 在可访问 VPCSession Manager 中所有实例的公司网络上部署 Linux 堡垒主机,
2. 在 EC2 实例上部署 AWS Systems Manager 代理.使用具有权限的用户访问权限来访问 EC2 实例
3. 在公共子网中部署具有弹性 IP 地址的 Linux 堡垒主机.允许访问 10 个堡垒主机 tom 0.0.0.0/0 D.建立将公司网络连接到 VPC 的站点到站点 VPN 更新安全组以仅允许从公司网络访问

答:D

Question 8

一家公司计划迁移到 AWS.解决方案架构师在整个团队中使用 AWS Application Discovery Service,并发现有一个 Oracle 数据仓库和几个 Postgresql 数据库.

哪种迁移模式组合可以减少许可成本和运营开销? (选择两个)

1. 使用 AWS DMS 将 Oracle 数据仓库提升并转移到 Amazon EC2
2. 使用 AWS SCT 和 AWS DMS 将 Oracle 数据仓库迁移到 Amazon Redshift
3. 使用 AWS DMS 将 Postgresql 数据库提升并转移到 Amazon EC2
4. 使用 AWS DMS 将 Postgresql 数据库迁移到 Amazon RDS for Postgresql
5. 使用 AWS DMS 将 Oracle 数据仓库迁移到 Amazon EMR 管理的集群答案:BD

Question 9

一家公司正在 Amazon EC2 上运行两层 Web 应用程序. Web 层由一个应用程序负载均衡器(ALB)组成, 该负载均衡器由跨多个可用区的 Web 服务器实例的 Auto Scaling 组支持.数据库层使用的是 Amazon Aurora MYSQL.该公司的安全团队已部署了 AWS WAF 并将其与 ALB 集成在一起,以防止对应用程序进行 SQL 注入攻击.

最近,据报道存在安全漏洞,攻击者能够从随机 IP 地址访问单个 Web 服务器和公司数据库.安全团队最终能够编写出更好的规则来匹配攻击者使用的 SQL 注入技术.

但是,从在 EC2 实例上运行的第三方安全代理成功检测到攻击到此过程大约花费了一个小时. 安全团队可以使用哪种策略来保护数据库和整个基础架构?

1. 将 Amazon Cloudfront 层添加到现有架构.修改 AWS WAF 关联以与 Cloudfront 而不是 ALB 集成.更改Web 层安全组,以仅允许来自 Cloudfront 的 IP 地址.使用 Lambda @ Edge 进行请求检查并阻止重复的可疑请求.
2. 配置第三方安全代理以调用 AWS Lambda 函数. Lambda 函数应首先检查 Web 层的 Autoscaling 组, 以确保存在多个正在运行的实例,如果存在,则停止并隔离 Web 服务器实例
3. 启用 Amazon Macie 并打开其与 Amazon EC2 和 Aurora MYSQL 数据库的集成.为安全团队创建可视仪表板.配置自动警报并定义 AWS Lambda 函数以通过修改 VPC 中的安全组来自动阻止检测到的攻击D.部署 Amazon Guardduty 以分析 VPC 流日志.配置 Amazon Eventbridge 规则,该规则在 Guardduty 警报时触发 AWS Lambda 函数.通过修改 VPC 中的安全组,将 Lambda 功能配置为自动阻止检测到的攻击

答:D

Question 10

一家公司在欧洲拥有一个移动应用程序.使用该应用程序时,它将下载特定于设备和应用程序版本的配置 文件.该公司具有以下架构:

-配置文件存储在 eu-west-1 区域的 Amazon S3 中,并提供给 Amazon Cloudfront 用户

-Lambda @ Edge 用于从应用程序请求中提取设备和版本信息.然后更新请求以加载正确的配置.

该公司使用配置文件加载时间作为关键性能指标,目标响应时间为 100 毫秒或更短.该应用程序最近在ap-southeast-2 Region 中启动,澳大利亚用户的请求延迟大大高于 100 毫秒目标.解决方案架构师需要推荐一个解决方案.

哪种解决方案可以减少澳大利亚用户的延迟?

1. 在 ap-southeast-2 区域中创建一个 S3 存储桶.使用跨区域复制从 eu-west-1 Region Modity 中的存储桶进行同步. Lambda @ Edge 访问最靠近用户的区域中的 Amazon S3
2. 在存储桶上配置 S3 传输加速.修改 Lambda @ Edge 以使用离用户最近的 Region 中的 Transfer Acceleration 终端节点访问Amazon S3.
3. 在存储桶上配置 S3 Transfer Acceleration.将澳大利亚和欧洲的 Transfer Acceleration Edge 端点添加为 Cloudfront 来源.修改 Lambda @ Edge 以将请求的来源更新为最接近用户的 Region 中的 Transfer Acceleration 端点
4. 在 ap-southeast-2 区域中创建一个 S3 存储桶.使用跨区域复制从 eu-west-1 区域中的存储桶进行同步创建 Amazon.路由 53 托管区域,为两个存储桶均配置了基于延迟的路由.修改 Lambda @ Edge 以将请求的来源更新为距离用户最近的 Route 53 托管区域.

答:C

Question 11

一家公司在北美和南美经营管道.该公司使用图像和超声波传感器数据评估管道检查仪表,以监视其管道状况.管道位于具有间歇性或不可用的互联网连接的区域.每个站点的图像数据每月需要1 TB 的存储空间. 该公司希望找到一种解决方案,以每月一次的间隔在每个站点收集数据,并以高持久性存储数据.必须对捕 获的图像进行预处理,然后将其上传到中心位置以进行持久存储.

解决方案架构师应采取哪些行动来满足这些要求?

1. 在集群配置中的本地站点上部署 AWS Snowball 设备将 AWS Lambda 配置为进行预处理将设备运送回最近的 AWS 区域并将数据存储在 Amazon S3 存储桶中
2. 在集群配置中的本地站点上部署 AWS Snowball Edge 设备.配置 AWS Lambda 进行预处理.将设备运回到最近的 AWS 区域并将数据存储在 Amazon S3 存储桶中
3. 在站点上的合格硬件上部署 AWS 很多 Greengrass.在设备上配置 AWS Lambda 进行预处理将处理后的数据上传到距离站点最近的 AWS 区域中的 Amazon S3 存储桶
4. 在站点上的合格硬件上部署 AWS 很多 Greengrass.在设备上配置 AWS Lambda 进行预处理.将设备运回到最近的 AWS 区域并将数据存储在 Amazon S3 存储桶中

答:D

Question 12

一家公司正在使用多个 AWS 账户. DNS 记录存储在帐户 A 中 Amazon Route 53 的专用托管区域中.该公司的应用程序和数据库在帐户 B 中运行.

解决方案架构师将在新的 VPC 中部署两层应用程序.为了简化配置,在 Amazon Route 53 的专用托管区域中创建了 Amazon RDS 端点的 db.example.com CNAME 记录集.

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

解决方案架构师应采取哪些步骤组合解决此问题?(选择两个)

1. 在新的 VPC 中的单独 EC2 实例上部署数据库.在私有托管区域中为实例的私有 IP 创建记录集
2. 使用 SSH 连接到应用程序层 EC2 实例.将 RDS 端点 IP 地址添加到/etc/resolv.conf 文件中
3. 创建一个授权,以将帐户 A 中的专用托管区域与帐户 B 中的新 VPC 关联
4. 在账户 B 中为 example.com 域创建一个私有托管区域.在 AWS 账户之间配置Route 53 复制
5. 将帐户 B 中的新 VPC 与帐户 A 中的托管区域相关联删除帐户 A 中的关联授权

答:AC

Question 13

解决方案架构师正在设计一个可公开访问的 Web 应用程序,该应用程序在 Amazon Cloudfront 发行版上, 以 Amazon 网站终端节点为源.部署解决方案后,网站将返回错误 403:访问被拒绝消息.

解决方案架构师应采取哪些步骤解决问题?(选择两个) A.从 S3 存储桶中删除 S3 块公共访问选项

1. 从 S3 存储桶中删除请求者付款选项
2. 从 Cloudfront 发行版本中删除原始访问身份(OAL)
3. 将存储类别从 s3 标准更改为 S3 一区不频繁访问(S3 One Zone-IA)
4. 禁用 S3 对象版本控制

答:AB

Question 14

公司要求所有内部应用程序连接使用私有 IP 地址.为了简化该策略,解决方案架构师创建了接口端点以连接到 AWS 公共服务.经过测试,解决方案架构师注意到服务名称正在解析为公共 IP 地址,并且内部服务无法连接到接口端点.

解决方案架构师应采取哪一步来解决此问题?

1. 用到接口端点的路由更新子网路由表
2. 在 VPC 属性上启用专用 DNS 选项
3. 在接口端点上配置安全组,以允许连接到 AWS 服务.
4. 使用内部应用程序的条件转发器配置 Amazon Route 53 私有托管区域

答:B

Question 15

一家电子商务公司拥有要迁移到 AWS 的订单处理应用程序.该应用程序的数据量模式不一致,但是需要始终可用.必须在订单发生时和收到订单时对其进行处理

解决方案架构师应采取哪些步骤来满足这些要求?

1. 将 AWS Transfer 用于 SFTP 并在订单出现时上载订单.使用多个可用区中的按需实例进行处理
2. 将 Amazon SNS 与 FIFO 一起使用,并在发生订单时发送订单.使用单个大型预留实例进行处理
3. 将 Amazon SQS 与 FIFO 一起使用,并在发生订单时发送订单.在多个可用区中使用预留实例进行处理
4. 将 Amazon SQS 与 FIFO 一起使用,并在发生订单时发送订单.使用多个可用区中的竞价型实例进行处理

答:C

Question 16

一家公司有一个 Web 应用程序,允许用户上传短视频.视频存储在 Amazon EBS 卷上,并通过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具有峰值.该架构由在 Web 应用程序的 Auto Scaling 组中运行的 Amazon EC2 实例和在 Auto Scaling 组中运行以处理 Amazon SQS 队列的 EC2 实例组成.

该公司希望使用 AWS 托管服务重新架构该应用程序,以减少运营开销.尽可能删除对第三方软件的依赖. 哪种解决方案符合这些要求?

1. 将 Amazon ECS 容器用于 Web 应用程序,将竞价型实例用于处理 SQS 队列的 Auto Scaling 组.用

Amazon Rekognition 替换自定义软件以对视频进行分类

1. 将上传的视频存储在 Amazon EFS 中,并将文件系统安装到 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

1. 将 Web 应用程序托管在 Amazon S3 中.将上传的视频存储在Amazon S3 中.使用 S3 事件通知将事件发布到 SQS 队列.使用 AWS lambda 函数处理 SQS 队列,该函数调用 Amazon Rekognition API 对视频进行分类
2. 使用 AWS Elastic Beanstalk 在 Web 应用程序的 Auto Scaling 组中启动 EC2 实例,并启动工作程序环境来处理 SQS 队列.用 Amazon Rekognition 替换自定义软件以对视频进行分类.

答:C

Question 17

解决方案架构师在 AWS 上设计要求 99.99%可用性的 Web 应用程序,该应用程序将由三层架构组成,该架构在遇到高峰流量时每分钟支持 3000,000 个 Web 请求.该应用程序将使用 Amazon Route 53 进行DNS 解析,作为内容交付网络(CDN)的 Amazon CloudFront,用于负载平衡的 Elastic Load Balancer,用于

扩展应用程序层的 Amazon EC2 Auto Scang 组以及作为后端数据库的 Amazon Aurora MySQL.后端数据库负载将平均读取 90%和 10%的写入.该公司希望提供一种经济高效的解决方案,但可靠性至关重要. 解决方案架构师应该使用哪些策略?

1. 在单个 AWS 区域中构建应用程序.使用 Auto Scaling 组将 EC2 应用程序层部署到三个可用区,并根据请求指标进行动态扩展.将多可用区 Amazon Aurora MySQL 数据库集群与两个 Aurora 副本一起使用.每个 Aurora 副本必须具有足够的容量以支持 50%的峰值读取查询.
2. 在单个 AWS 区域中构建应用程序.使用 Auto Scaling 组将 EC2 应用程序层部署到三个可用区,最小所需容量足以每分钟处理 450,000 个请求.使用具有两个Aurora 副本的多可用区 Amazon Aurora MYSQL DB 群集每个 Aurora 副本必须具有足够的容量以支持 100%的峰值读取查询.
3. 在单个 AWS 区域中构建应用程序.使用 Auto Scaling 组将 EC2 应用程序层部署到两个可用区,其最小所需容量足以每分钟处理 30.0000 个请求,使用具有一个 Aurora 副本的Multi-az Amazon Aurora MYSQL DB 集群. Aurora 副本必须具有足够的容量以支持峰值读写查询的 50%.
4. 在两个 AWS 区域中构建应用程序.使用 Auto Scaling 组将 EC2 应用程序层部署到两个可用区,并根据第二个区域中每个区域中的请求指标进行动态扩展,部署 Amazon Aurora MYSQL 跨区域副本,使用Amazon Route 53 在区域之间分配流量,如果区域不可用,请配置故障转移

答:B

Question 18

公司使用负载均衡器将流量分配到单个可用区中的 Amazon EC2 实例.该公司对安全性深信不疑,并希望解决方案架构师重新设计解决方案以满足以下要求

-必须过滤入站请求以进行常见漏洞攻击

-被拒绝的请求必须发送到第三方审核应用程序

-所有资源应高度可用

哪种解决方案符合这些要求?

1. 使用应用程序 AMI 配置 Multi-az Auto Scaling 组创建应用程序负载平衡器(ALB),然后选择先前创建的Auto Scaling 组作为目标.使用 Amazon Inspector 监视到 ALB 和 EC2 实例的流量.在 WAF 中创建 Web ACL 使用 Web ACL 和 ALB 创建 AWS WAF.使用 AWS Lambda 函数经常将 Amazon Inspector 报告推送到第三方审核应用程序
2. 配置一个应用程序负载平衡器(ALB)并将 EC2 实例添加为目标,在 WAF 中创建一个 Web ACL 使用Web ACL 和 ALB 名称创建一个 AWS WAF,并启用 Amazon Cloudwatch Logs 的日志记录.使用 AWS Lambda 函数将日志频繁推送到第三方审核应用程序
3. 配置一个应用程序负载平衡器(ALB)以及一个将 EC2 实例添加为目标的目标组.使用第三方审核应用程序的目的地创建 Amazon Kinesis Data Firehose.在 WAF 中创建 Web ACL 使用 Web,ACL 和 ALB 创建AWS WAF,然后通过选择 Kinesis Data Firehose 作为目标来启用日志记录.在 AWS Marketplace 中订阅AWS Managed Rules,选择 WAF 作为订阅者
4. 使用应用程序 AML 配置 Multi-az Auto Scaling 组.创建一个应用程序负载平衡器(ALB),然后将先前创建的 Auto Scaling 组作为目标.创建带有第三方审核应用程序目标的 Amazon Kinesis Data Firehose.在WAF 中创建 Web ACL 使用 WebACL 和 ALB 创建一个 AWS WAF,然后通过选择 Kinesis Data Firehose 作为目的地来启用日志记录在 AWS Marketplace 中订阅AWS 受管规则,然后选择 WAF 作为订阅者.

答:D

Question 19

公司由多个开发团队共同致力于多个项目.开发人员经常在项目之间移动,并且每个项目都需要访问不同 的 AWS 资源集.

当前有用于 Web,移动和数据库开发的项目.项目集可能会随着时间而改变.

开发人员应完全控制分配给他们的项目的资源,并对所有其他项目的资源具有只读权限.

将开发人员分配给其他项目或添加新的 AWS 资源时.公司要维护. 解决方案架构师应建议哪种控制策略?

1. 为每个项目创建带有特定项目标签的策略文档,并使用匹配的标签允许对资源的完全控制.允许对所有其他资源进行只读访问.将特定于项目的策略文档附加到该项目的 IAM 角色.当他们更改项目时,更改分配给开发人员的 IAM 用户的角色.创建新资源时,将特定项目标签分配给新资源
2. 为每个需要访问 AWS 资源的项目创建一个 IAM 角色.在角色上附加一个内联策略文档,该文档指定允许承担该角色的 AM 用户,并完全控制属于项目的资源,并且只读访问帐户中所有其他资源的权限.资源集变更或开发人员变更项目
3. 创建一个客户管理层为需要访问 AWS 资源的每个项目指定完全控制策略文档.指定对项目资源的完全控制,并指定帐户中所有其他资源的只读权限.当开发人员更改项目时,将特定于项目的策略文档附加到开发人员的 IAM 用户.资源集更改时更新策略文档
4. 为每个需要访问 AWS 资源的项目创建一个客户管理策略文档,指定对属于该项目的资源的完全控制,并对帐户中所有其他资源进行只读访问,将特定于项目的策略文档附加到 IAM 组当开发人员的更改项目时更改组成员身份.当对资源的设置更改时,更新策略文档.

答:D

Question 20

一家公司计划将整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:

-它应该允许每小时发布几次更改

-它应该能够尽快回滚更改.

哪种设计可以满足这些要求?

A.部署包含 Aml 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. B.指定要在辅助环境中暂存的 AWS Elastic Beanstalk 作为 CLCD 应用程序管道的部署目标.部署,交换过渡和生产环境 URL.

1. 使用 AWS Systems Manager 重新配置每个部署的基础架构更新 Amazon EC2 用户数据以从

Amazon S3 中获取最新的代码工件,并使用 Amazon Route 53 加权路由来指向新环境.

1. 使用预建的 AMI 将应用程序更新作为自动扩展事件的一部分进行.使用 Amls 的新版本添加实例,并在部署事件期间逐步淘汰所有使用先前 AMI 版本和已配置终止策略的实例.

答:B

Question 21

解决方案架构师正在将现有工作负载迁移到 AWS Fargate.该任务只能在 VPC 内的私有子网中运行,该私有子网没有从系统外部到应用程序的直接连接.启动 Fargate 任务时,该任务失败,并显示以下错误: CannotPullcontainererror:API 错 误 (500):Gethttp:/111122223333.dkr.ecr.us-east- 1.amazonaws.com/v2/net/http:等待连接时请求已取消

解决方案架构师应如何纠正此错误?

1. 确保在启动任务时将任务设置为 ENABL ED 以进行自动分配的公共 IP 设置
2. 确保在启动任务时将任务设置为 DISABLED 以自动分配公共 IP 设置.在 VPC 的公共子网中配置 NAT

网关以将请求路由到 Internet

1. 确保启动任务时将任务设置为 DISABL ED 以进行自动分配公共 IP 设置.在 VPC 的专用子网中配置NAT 网关以将请求路由到 Internet
2. 确保在 Fargate 任务定义中将网络模式设置为桥接

答:B

Question 22

公司有照片共享社交网络应用程序.为用户提供一致的体验.该公司会对用户上传的照片进行一些图像处 理,然后再发布到应用程序上.图像处理使用一组 Python 库实现.

当前的体系结构如下.

-图像处理 Python 代码在单个 Amazon EC2 实例中运行,并将处理后的图像存储在名为 Imagebucket 的

Amazon s3 存储桶中.

-托管在另一个存储桶中的前端应用程序从 Imagebucket 加载图像以显示给用户.

通过全球扩展计划,该公司希望对现有体系结构进行更改,以便能够扩展对应用程序的需求,并降低应用程 序规模带来的管理复杂性.

不久就要进行哪些变更组合?(选择两项)

1. 将图像处理 EC2 实例放置到 Auto Scaling 组中.
2. 使用 AWS Lambda 运行图像处理任务
3. 使用 Amazon Rekognition 进行图像处理
4. 在 Imagebucket 之前使用 Amazon Cloudfront
5. 在 Amazon ECS 容器中部署应用程序并应用服务自动扩展

答案:BD

Question 23

公司使用 AWS 组织和一个名为 Production 的 OU 来管理多个账户.所有账户都是 Production OU 的编号. 管理员使用组织中的拒绝列表 SCP 来管理对受限服务的访问.

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. 删除限制访问 AWS Config 的组织的根 SCP.创建适用于公司标准 AWS Config 规则的AWS Service Catalog 产品,并将其部署到整个组织中,包括新帐户
2. 为新帐户创建一个名为 Onboarding 的临时OU 将 SCP 应用于Onboarding OU 以允许 AWS Config

操作.完成对AWS Config 的调整后,将新帐户移至 Production OU

1. 将组织的根 SCPS 从拒绝列表 SCPS 转换为下列表 SCPS,以仅允许所需的服务.将 SCP 临时应用到组织根目录,该根目录仅允许新帐户中的委托人执行 AWS Config 操作.
2. 为新帐户创建一个名为 Onboarding 的临时 ou.将 SCP 应用于Onboarding OU 以允许AWS Config 操作.将组织的根 SCP 移到生产 OU 中,完成对 AWS Config 的调整后,将新帐户移到生产 OU 中

答:D

Question 24

一家公司在其数据中心中拥有一个 Microsoft SQL Servor 数据库,并计划将数据迁移到 Amazon Aurora MySQL.该公司已经使用 AWS Schema Conversion Tool 将触发器,存储过程以及其他架构对象迁移到Aurora MySQL.数据库包含 1TB 数据,并且每天增长不到 1 MB.

该公司的数据中心通过专用的 1 Gbps AWS Direct Connect 连接连接到 AWS.

该公司希望通过 Aurora MySQL 迁移数据,并以最少的停机时间对应用程序进行重新配置.

哪种解决方案符合公司的要求?

答:在周末关闭应用程序.创建一个 AWS DMS 复制实例和任务以将现有数据从 SQL Server 迁移到

Aurora MYSQL 执行应用程序测试并将数据迁移到新的数据库终端节点

1. 创建一个 AWS DMS 复制实例和任务以将现有数据和正在进行的复制从 SQL Server 迁移到 Aurora MYSQL 执行应用程序测试并将数据迁移到新的数据库端点
2. 在 Amazon S3 上创建SOL Server 的数据库快照.将数据库快照从 Amazon S3 还原到 Aurora MYSQL. 创建一个 AWS DMS 复制实例和任务,以进行从 SQL Server 到 Aurora MYSQL 的持续复制.执行应用程序测试并将数据迁移到新的数据库端点.
3. 在 Amazon S3 上创建一个 SQL Server 本机备份文件.创建一个 AWS DMS 复制实例和任务,以将SQL Server 备份文件还原到 Aurora MYSQL；另一个 AWS DMS 任务,用于从 SQL Server 到 Aurora MYSQL 的持续复制.执行应用程序测试,并将数据迁移到新的数据库端点.

答:B

Question 25

某金融服务公司从其信用卡服务合作伙伴处接收到可再生数据提要,每 15 分钟以明文形式发送约 5,000 条记录,并通过 HTTPS 直接将其发送到具有服务器端加密的 Amazon S3 存储桶中,此提要包含敏感的信用卡主帐号(PAN)数据,公司需要先自动屏蔽 PAN,然后再将数据发送到另一个 S3 存储桶以进行其他内部处理,该公司还需要删除并合并特定字段,然后将记录转换为 JSON 格式.此外,额外的提要可能会在将来出现,因此任何设计都必须易于扩展.

有哪些解决方案可以满足这些要求?

1. 在文件交付时触发 Aws Lambda 函数,该函数提取每条记录并将其写入 Amazon SQS 队列.当新消息到达此队列中时,将触发另一个 Lambda 函数以处理记录,并将结果写入 Amazon S3 中的术语表位置.一旦sqs 队列有效,就触发最终的 Lambda 函数,以将记录转换为 JSON 格式并将结果发送到另一个 S3 存储桶以进行内部处理
2. 在文件交付时触发 Aws Lambda 函数,该函数提取每条记录并将其写入 Amazon SQS 队列.当 SQS 队列包含消息时,将 AWS Fargate 容器应用程序配置为自动联盟扩展为单个实例.让应用程序处理每个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 存储桶以进行内部处理,并按比例缩小 AWS Fargate 实例
3. 基于数据馈送格式创建 AWS Glue 搜寻器和自定义分类器,并构建与之匹配的表定义触发 AWS Lmbda 函数场以启动 AWS Glue ETL 作业以根据处理和转换要求转换整个记录输出格式为 JSON 一旦完成,请让 Etljobs 将结果发送到另一个 S3 存储桶以进行内部处理
4. 根据数据格式创建 Aws Glue 狂热者和自定义分类,并建立匹配的表定义.对 Amazon Athena 进行文件传递查询,以启动 Amazon EMR ETL 作业,以根据处理和转换整个记录转换要求.将输出格式定义为JSON.完成后将结果发送到另一个 S3 另一个 S3 存储桶以进行内部处理并缩减 EMR 集群.

答:A

Question 26

一家公司正在将其应用程序手动部署到生产中,并希望转向更成熟的部署模式.该公司已要求解决方案架构师设计一种利用其当前的 Chef 工具和知识的解决方案.在部署到生产环境之前,必须将应用程序部署到暂存环境中进行测试和验证.如果在部署后发现错误,则必须在 5 分钟内回滚任何新的部署

解决方案架构师应使用哪种 AWS 服务和部署模式来满足这些要求?

1. 使用 AWS Elastic Beanstalk 并使用所有更新部署策略来部署应用程序
2. 使用 AWS Codepipeline 并使用 rolin 更新部署状态部署 aplicaton
3. 使用 Aws Codebuild 并使用 canary deploymen sreley 部署 Apicaion
4. 使用 AWS OpsWorks 并使用蓝/绿部署策略部署应用程序

答:D

Question 27

解决方案架构师正在为公司的移动应用程序用户实施对 AWS 的联合访问.由于法规和安全要求,应用程序必须使用定制解决方案来对用户进行身份验证,并且必须使用AM 角色进行授权.

以下哪些操作将启用身份验证和授权并满足要求?(选择两个)

1. 使用定制的 SAML 兼容解决方案进行身份验证,并使用AWS SSO 进行授权.
2. 使用 Amazon API Gateway 和 AWS Lambda 进行身份验证来创建定制的 LDAP 连接器.将授权令牌存储在 Amazon Dynamodb 中,并使用另一个从 Lambda 函数读取 Dynamodb 凭据的 Lambda 函数来验证授权请求
3. 使用定制的 OpenID Connect 兼容解决方案和 AWS SSO 进行身份验证和授权.
4. 使用定制的与 Saml 兼容的解决方案,该解决方案使用 LDAP 进行身份验证并使用 SAML 断言对 LAM

身份提供程序执行授权.

1. 使用定制的兼容 Opend Connect 的解决方案进行身份验证,并使用Amazon Cognito 进行授权

答:AE

Question 28

一本在线杂志将于本月发行最新版本.该版本将是第一个在全球发行的版本.该杂志的动态网站当前在Web 层前面使用 Application Load Balancer,用于 Web 和应用程序服务器的 Amazon EC2 实例队列以及Amazone Aurora MySQL.静态内容,几乎所有流量都是只读的.

解决方案架构师应采取哪些步骤组合来减少全球受众的系统响应时间? (选择两个)

1. 使用逻辑跨区域复制将 Aurora MYSQL 数据库复制到辅助区域,用 Amazon S3 替换 Web 服务器以跨区域复制模式部署 S3 存储桶
2. 确保 Web 和应用程序层都在 Auto Scaling 组中.引入 AWS Direct Connect 连接在全球区域中部署

Web 和应用程序层

1. 将数据库从 Amazon Aurora 迁移到 Amazon RDS for MYSQL,确保所有三个应用程序层(Web,应用程序和数据库)都在专用子网中\
2. 使用 Aurora 全局数据库进行物理跨区域复制.将 Amazon S3 与跨区域替换一起用于静态内容和资源. 在世界各地的区域中部署 Web 和应用程序层.
3. 将 Amazon Route 53 引入基于延迟的路由和 Amazon Cloudfront distr,然后再打开.确保 Web 和应用程序层分别在 Auto Scaling 组中

答:DE

Question 29

一家公司在 ap-southeast-2 区域中的应用程序负载平衡器(ALB)后面部署了基于 Web 的应用程序.AWS 证书管理器(ACM)已颁发 TLS 证书(例如 com).该证书已部署到 ALB. Amazon Route 53 中有一个与ALB 相关的记录集,例如 com.

由于应用程序负载增加,该公司希望使用 Amazon Cloudfront.此转换不会导致应用程序停机.

哪种行动组合可以实现这一目标? (选择三项)

1. 在 ap-southeast2 区域中为源 example.com 和 examplecom 创建一个新的 ACM 证书.将此证书与现有的 ALB 相关联.在 Route 53 中为与现有 ALB 关联的 origin.example.com 添加 DNS 条目
2. 创建一个 Cloudfront 发行版,并使用与 ap-southeast-2 区域中的 ALB 关联的现有证书将源示例 com 作为自定义源
3. 在美国东部 1 地区(例如 com)创建一个新的 ACM 证书.创建一个 Cloudfront 发行版,并在 us east-1 Region 中使用 ACM 证书.将来源示例 com 设置为自定义 ongin.
4. 将 Route 53(例如 com)更新为 Cloudfront 发行版本的别名记录
5. 在美国东部 1 地区为 example.com 创建一个新的 ACM 证书.在 us-ast-1 区域中创建一个新的 ALB 作为 Cloudfront 分发的来源将与 ALB 关联的安全组附加到 Cloudfront 分发
6. 更新 ALB 安全组以仅允许从 Cloudfront Edge 位置进行访问

答:CDF

Question 30

移动应用程序已变得非常流行,使用量已从几百个增加到数百万个用户.用户捕获并上传城市内活动的图像,并提供评级和建议数据访问方式是无法预测的.当前应用程序托管在 Application Load Balancer(ALB) 之后的 Amazon EC2 实例上.该应用程序正经历速度下降,成本快速增长

解决方案架构师应对应用程序体系结构进行哪些更改以控制成本并提高性能?

1. 创建一个 Amazon Cloudfront 发行版并将 ALB 放在发行版后面.在不频繁访问存储类中将静态内容存储在 Amazon S3 中
2. 使用 Intelligent Tiering 存储类将静态内容存储在 Amazon S3 存储桶中.在 S3 存储桶和 ALB 之前使用

Amazon Cloudfront 发行版

1. 将 AWS Global Accelerator 放在 ALB 的前面.将静态内容迁移到 Amazon EFS,然后运行 AW Lambda

函数以在迁移过程中调整图像的大小

1. 将应用程序代码移至 AWS Fargate 容器,并用 Fargate 容器交换 EC2 实例.

答:A **建议选项：B**

Question 31

一家公司希望在 AWS 上运行无服务器应用程序该公司计划在 Amazon ECS 集群中运行的 Docker 容器中配置其应用程序该应用程序需要 MYSQL 数据库,并且该公司计划使用 Amazon RDS 该公司的文档需要经常访问前三个月,此后很少.文件必须保存多年.

满足这些要求的最具成本效益的解决方案是什么?

1. 使用按需实例创建 ECS 集群使用竞价型实例在 Amazon RDS 中置备数据库及其只读副本.将文档存储在加密的 EBS 卷中,并创建 cron 作业以在 7 年后删除文档.
2. 使用一组竞价型实例创建 ECS 集群,并启用竞价型实例排空功能.使用预留实例在 Amazon RDS 中设置数据库及其只读副本.将文档存储在具有生命周期策略的安全 Amazon S3 存储桶中,以将 3 个月以上的文档移至 Amazon S3 Glacier.然后从 Amazon S3 Glacier 中删除已使用 7 年以上的文档
3. 使用按需实例创建 ECS 集群使用按需实例在 Amazon RDS 中置备数据库及其只读副本.将文档存储在Amazon EFS 中创建一个 cron 作业,将早于几个月的文档移至 Amazon S3 Glacier.创建一个 AWS Lambda 函数以删除 S3 Glacier 中 7 年以上的文档
4. 使用已启用竞价型实例排空的竞价型实例创建 ECS 集群.使用按需实例在 Amazon RDS 中设置数据库及其只读副本.将文档存储在具有生命周期策略的安全 Amazon S3 存储桶中,以将 3 个月以上的文档移至Amazon S3 Glacier,并在 7 年后删除 Amazon S3 Glacier 中的文档

答:B

Question 32

解决方案架构师必须启用 N 个访问控制的 AWS Cloudhsm M(也称为法定身份验证机制),以允许安全人员对硬件安全模块(HSM)进行管理更改.新安全策略规定,这五个中的至少三个安全员必须授权对CloudHSM 进行任何管理更改.

哪种结构合理的设计可确保安全人员可以通过仲裁?

1. 在与 Amazon API Gateway 集成的Amazon S3 上创建一个静态网站,以允许人员启动法定请求.使用Amazon SNS 通知法定请求的官员.允许警官下载Cloudhsm 仲裁令牌,脱机签名令牌并通过网站上传已签名的令牌.使用 Amazon Dynamodb 存储仲裁令牌和其他人员的响应以及他们的已签名的仲裁令牌.配置 AWS Step Functions 工作流程以编排人员通知,在 Amazon Dynamodb 中对已签名令牌进行计数,并在至少三名人员签署令牌后通知发起人员.使用签名的仲裁令牌来管理 CloudHSM.
2. 在与 Amazon API Gateway 集成的Amazon S3 上创建一个静态网站,以允许人员启动仲裁请求.使用网站重定向人员,以其联盟身份凭证登录 Cloudhsm.一旦至少三名官员登录到 CloudHSM.启动同步仲裁令牌签名过程.使用签名的仲裁.用于管理 CloudHSM 的令牌.
3. 创建一个在应用程序负载平衡器后面的多个 Amazon EC2 实例上托管的仲裁签名应用程序,以允许管理人员发起仲裁请求.要求官员使用其联合身份凭证登录到应用程序.然后,每个人员将使用该应用程序批 准仲裁签名请求.将应用程序配置为使用 AWS STS 代表管理人员签署 CloudHSM 仲裁令牌.一旦至少三名官员批准了仲裁签名请求,就可以使用 EC2 IAM 服务角色来使用签署的仲裁令牌来管理 Cloudhsm.
4. 使用 AWS Lambda 代理集成创建经过 Amazon Cognito 身份验证的 Amazon API Gateway API 终端节点.使用 Amazon Cognito 登录后,允许官员创建Cloudhsm 仲裁令牌并将其发布到 API Gateway API. 使用管理员的 Amazon Cognito IAM 角色,配置 Lambda 函数以对仲裁令牌执行签名过程,并将签名后的令牌存储在 Amazon Dynamodb 中.一旦至少三名官员签署了法定令牌,请允许 POST 方法使用已签署的令牌来管理 Cloudhsm

答:D

Question 33

一家公司正在使用现有的业务流程管理工具来管理数千个 Amazon EC2 实例.最近的渗透测试在该公司的软件堆栈中发现了一个漏洞,该漏洞促使该公司对其当前的生产环境进行全面评估.分析确定环境中存在以下漏洞.

-生产中正在使用具有过时的库和已知漏洞的操作系统.

-由公司托管和管理的关系数据库正在运行不受支持的具有已知漏洞的版本

-存储在数据库中的数据未加密.

解决方案架构师打算使用 AWS Config 持续审核和评估公司的 AWS 资源配置是否符合公司的政策和准则.哪些额外的步骤将使公司在遵循最佳实践的同时保护环境并跟踪资源?

1. 使用 AWS Application Discovery Service 评估所有正在运行的 EC2 实例.使用 Aws CLI 对每个实例进行修改,并使用 EC2 用户数据在引导计划修补期间安装 AWS Systems Manager Agent,以作为 Systems Manager 维护 Windows 任务运行.将所有关系数据库迁移到 Amazon RDS 并启用 AWS KMS 加密
2. 为 EC2 实例创建一个 AWS Cloudformation 模板.在 Cloudformation 模板中使用 EC2 用户数据来安装AWS Systems Manager 代理,并在所有 Amazon EBS 卷上启用 AWS KMS 加密.让 Cloudformation 替换所有正在运行的实例.使用 Systems Manager Patch Manager 建立补丁程序基准并部署系统管理维护Windows 任务以使用补丁程序基准执行 Aws-runpatchbaseline
3. 使用公司当前的编排工具在所有现有实例上安装 AWS Systems Manager Agent.使用 Systems Manager 运行命令来执行命令列表,以使用特定于操作系统的工具在每个实例上升级软件.在所有Amazon EBS 卷上启用 AWS KMS 加密.
4. 使用该公司当前的编排工具在所有现有实例上安装 AWS Systems Manager Agent.将所有关系数据库迁移到 Amanzon RDS 并启用 AWS KMS 加密.使用 Systems Manager Patch Manager 建立补丁程序基准并部署 Systems Manager 维护 Windows 任务以使用补丁程序基准执行 AWS-Run-PatchBaseline.

答:D

Q34

A company has many services running in its on-premises data center.The data center is connected to AWS using AWS Direct Connect(DX)and an Ipsec VPN The service data is sensitive and connectivity cannot traverse the internet The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS

Which solution will meet these requirements?

A.Create a VPC Endpoint Service that accepts TCP trafic , host it behind a Network Load Balancer and make the service available over DX

B.CreateaVPCEndpointServicethatacceptsHTTPorHTTPStraffichostitbehindanApplication Load Balancer, and make the service available over DX

C.Attach an internet gateway to the VPC , and ensure that network access control and security group rules allow the relevant inbound and outbound traffic

D.Attach a NAT gateway to the VPC , and ensure that network access control and security group rules allow the relevant inbound and outbound traffic

Answer: A

某公司在其本地数据中心中运行着许多服务。该数据中心使用AWS Direct Connect（DX）和Ipsec VPN连接到AWS服务数据很敏感且连接无法穿越互联网公司希望扩展到 新的细分市场，并开始向使用AWS的其他公司提供服务

哪种解决方案可以满足这些要求？

A.创建一个接受TCP流量的VPC端点服务，将其托管在网络负载平衡器之后，并通过DX使该服务可用

B.在应用程序负载均衡器后面创建一个接受HTTP或HTTPStraffichost的VPCEndpointService，并通过DX使该服务可用

C.将Internet网关连接到VPC，并确保网络访问控制和安全组规则允许相关的入站和出站流量

D.将NAT网关连接到VPC，并确保网络访问控制和安全组规则允许相关的入站和出站流量

答：A

Q35

A company has a VPC with two domain controllers running Active Directory in the default configuration. The VPC DHCP options set is configured to use the IP addresses of the two domain controllers. There is a VPC interface endpoint defined; but instances within the VPC are not able to resolve the private endpoint addresses.

Which strategies would resolve this issue? (Choose two.)

A.Define an outbound Amazon Route 53 Resolver.

Set a conditional forward rule for the Active Directory domain to the Active Directory servers.

Update the VPC DHCP options set to AmazonProvidedDNS.

B.Update the DNS service on the Active Directory servers to forward all non-authoritative queries to the VPC Resolver.

C.Define an inbound Amazon Route 53 Resolver.

Set a conditional forward rule for the Active Directory domain to the Active Directory servers.

Update the VPC DHCP options set to AmazonProvidedDNS.

D.Update the DNS service on the client instances to split DNS queries between the Active Directory servers and the VPC Resolver.

E.Update the DNS service on the Active Directory servers to forward all queries to the VPC Resolver.

Answer: AB

一家公司有一个VPC，其中有两个在默认配置下运行Active Directory的域控制器。 VPC DHCP选项集配置为使用两个域控制器的IP地址。定义了一个VPC接口端点；但是VPC内的实例无法解析私有端点地址。

哪些策略可以解决此问题？ （选择两个。）

A.定义出站Amazon Route 53解析程序。

将Active Directory域的条件转发规则设置为Active Directory服务器。

将VPC DHCP选项设置更新为AmazonProvidedDNS。

B.更新Active Directory服务器上的DNS服务，以将所有非权威性查询转发到VPC解析器。

C.定义入站Amazon Route 53解析器。

将Active Directory域的条件转发规则设置为Active Directory服务器。

将VPC DHCP选项设置更新为AmazonProvidedDNS。

D.更新客户端实例上的DNS服务，以在Active Directory服务器和VPC解析器之间拆分DNS查询。

E.更新Active Directory服务器上的DNS服务，以将所有查询转发到VPC解析器。

答：AB

Q36

A fitness tracking company serves users around the world , with its primary markets in North America and Asia.The company needs to design an infrastructure for its read-heavy user authorization application with the following requirements

-Be resilient to problems with the application in any Region

-Write to a database in a single RegionRead from multiple Regions

・ Support resiliency across application tiers in each Region

-Support the relational database semantics reflected in the application

Which combination of steps should a solutions architect take?(Select TWO)

A.Use an Amazon Route 53 geoproximiy outing policy combined with a multivalue answer routing policy

B.Deploy web , application , and MYSQL database servers to Amazon EC2 instances in each Region Set up the application so that reads and writes are local to the Region Create snapshots of the web application , and database servers and store the snapshots in an Amazon S3 bucket in both Regions Set up cross-region replication for the database laye

C Use an Amazon Route 53 geolocation routing policy combined with a failover routing policy D.Set up web , application , and Amazon RDS for MYSQL instances in each Region.Set up the

application so that reads are local and writes are partitioned based on the user.Set up a Multi-az failover for the web.application and database servers.Set up cross-region replication for the database layer.

E Set up active-active web and application servers in each Region Deploy an Amazon Aurora global database with clusters in each Region Set up the application to use the in-region Aurora database endpoints.Create snapshots of the web and application servers and store them in an Amazon S3 bucket in both Regions.

Answer: CE

一家健身追踪公司主要为北美和亚洲的主要市场服务于世界各地的用户，该公司需要为满足以下要求的重载用户授权应用程序设计基础架构

-抵御任何地区的应用程序问题

-在单个Region中写入数据库从多个Region读取

・支持每个地区的应用程序层之间的弹性

-支持应用程序中反映的关系数据库语义

解决方案架构师应采取哪些步骤组合？（选择两个）

A.结合使用Amazon Route 53地理接近郊游策略和多值答案路由策略

B.将Web，应用程序和MYSQL数据库服务器部署到每个区域中的Amazon EC2实例设置应用程序，以便对区域本地进行读写操作创建Web应用程序和数据库服务器的快照并将快照存储在Amazon S3中两个区域中的存储桶为数据库布局设置跨区域复制

C将Amazon Route 53地理位置路由策略与故障转移路由策略结合使用

D.在每个区域中为MYSQL实例设置web，应用程序和Amazon RDS。

应用程序，以便在本地进行读取，并根据用户对写入进行分区。为web.application和数据库服务器设置Multi-az故障转移。为数据库层设置跨区域复制。

E在每个区域中设置主动-主动式Web服务器和应用程序服务器在每个区域中部署具有群集的Amazon Aurora全局数据库设置应用程序以使用区域内Aurora数据库终端节点。创建Web和应用程序服务器的快照并将其存储在两个区域中都有一个Amazon S3存储桶。

答：CE

Q37

A company is planning on hosting its ecommerce platform on AWS using a multi-tier web application designed for a NoSQL database. The company plans to use the us-west-2 Region as its primary Region. The company wants to ensure that copies of the application and data are available in second Region, us- west-1, for disaster recovery. The company wants to keep the time to fail over as low as possible. Failing back to the primary Region should be possible without administrative interaction after the primary service is restored.

Which design should the solutions architect use?

A.Use AWS CloudFormation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers.

Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us- west-1 in the event of an outage.

Use Amazon DynamoDB global tables for the database tier.

B.Use AWS CloudFormation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers.

Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us- west-1 in the event of an outage Deploy an Amazon Aurora global database for the database tier.

C.Use AWS Service Catalog to deploy the web and application servers in both Regions Asynchronously

replicate static content between the two Regions using Amazon S3 cross-Region replication.

Use Amazon Route 53 health checks to identify a primary Region failure and update the public DNS entry listing to the secondary region in the event of an outage.

Use Amazon RDS for MySQL with cross-Region replication for the database tier.

D.Use AWS CloudFormation StackSets to create the stacks in both Regions using Auto Scaling groups for the web and application tiers.

Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use Amazon CloudFront with static files in Amazon S3, and multi-Region origins for the front-end web tier.

Use Amazon DynamoDB tables in each Region with scheduled backups to Amazon S3. Answer: A

一家公司计划使用专为NoSQL数据库设计的多层Web应用程序将其电子商务平台托管在AWS上。该公司计划将us-west-2地区用作其主要地区。该公司希望确保该应用程序和数据的副本在us-1的第二个区域中可用，以进行灾难恢复。该公司希望使故障转移的时间尽可能短。恢复主要服务后，无需管理交互就可以返回到主要区域。

解决方案架构师应使用哪种设计？

A.使用AWS CloudFormation StackSets在两个区域中为Web和应用程序层创建具有Auto Scaling组的堆栈。

使用Amazon S3跨区域复制在区域之间异步复制静态内容。如果发生故障，请使用Amazon Route 53 DNS故障转移路由策略将用户定向到us-west-1中的辅助站点。

将Amazon DynamoDB全局表用于数据库层。

B.使用AWS CloudFormation StackSets在两个区域中使用Web和应用程序层的Auto Scaling组创建堆栈。

使用Amazon S3跨区域复制在区域之间异步复制静态内容。发生故障时，请使用Amazon Route 53 DNS故障转移路由策略将用户定向到uswest-1中的辅助站点。为数据库层部署Amazon Aurora全局数据库。

C.使用AWS Service Catalog在两个区域中异步部署Web和应用程序服务器

使用Amazon S3跨区域复制在两个区域之间复制静态内容。

使用Amazon Route 53运行状况检查来识别主要区域故障，并在发生故障时将公共DNS条目列表更新到次要区域。

将Amazon RDS for MySQL与跨区域复制一起用于数据库层。

D.使用AWS CloudFormation StackSet在Web和应用程序层使用Auto Scaling组在两个区域中创建堆栈。

使用Amazon S3跨区域复制在区域之间异步复制静态内容。将Amazon CloudFront与Amazon S3中的静态文件以及前端Web层的多区域来源一起使用。

将每个区域中的Amazon DynamoDB表与到Amazon S3的计划备份一起使用。

答：A

Q38

A company wants to host a global web application on AWS. It has the following design requirements： -The access pattern must allow for fetching data from multiple data sources

-minimize the cost of API calls

-Keep page load times to within 50 ms

-Provide user authentication and authorization and manage data access for different user -personas (for example, administrator, anager, or engineer)

-use a serverless design

Which set of strategies should a solutions architect use?

A.Use Amazon Cloudfront with Amazon S3 to host the web application. Use Amazon API Gateway to build the application Apis with AWS Lambda for the custom authorizer. Authorize data access by performing user lookup in Simple AD.

B.Use Amazon Cloudfront with AWS WAF to host the web application. Use AWS Appsync to build the application APIS. Use LAM groups for each user persona. Authorize data access by leveraging LAMgroups in AWS AppSync resolvers

C.Use Amazon Cloudfront with Amazon S3 to host the web application. Use AWS Appsync to build the application Apis. Use Amazon Cognito groups for each user persona. Authorize data access by leveraging Amazon Cognito groups in AWS AppSync resolvers

D.Use AWS Direct Connect with Amazon S3 to host the web application. Use Amazon API Gateway to build the application Apis. Use AWS Lambda for custom authentication and authorization Authorize data access by leveraging LAM roles

Answer:A

一家公司希望在AWS上托管一个全球Web应用程序。它具有以下设计要求：-访问模式必须允许从多个数据源获取数据

-最小化API调用的费用

-将页面加载时间保持在50毫秒内

提供用户身份验证和授权，并管理不同用户角色（例如，管理员，anager或工程师）的数据访问

-使用无服务器设计

解决方案架构师应使用哪种策略？

答：将Amazon Cloudfront与Amazon S3结合使用以托管Web应用程序。使用Amazon API Gateway为定制授权者使用AWS Lambda构建应用程序Apis。通过在Simple AD中执行用户查找来授权数据访问。

B.结合使用Amazon Cloudfront和AWS WAF托管Web应用程序。使用AWS Appsync构建应用程序APIS。对每个用户角色使用LAM组。通过利用AWS AppSync解析器中的LAMgroup授权数据访问

C.结合使用Amazon Cloudfront和Amazon S3托管Web应用程序。使用AWS Appsync构建应用程序Apis。对每个用户角色使用Amazon Cognito组。通过利用AWS AppSync解析器中的Amazon Cognito组来授权数据访问

D.使用带有Amazon S3的AWS Direct Connect托管Web应用程序。使用Amazon API Gateway构建应用程序Apis。使用AWS Lambda进行自定义身份验证和授权通过利用LAM角色授权数据访问

答：A

Q39.

A startup company recently migrated a large ecommerce website to AWS The website has experienced a 70% increase in sales

Sofware engineers are using a private Github repository to manage code.The devops team is using Jenkins for builds and unit testing

The engineers need to receive notifications for bad builds and zero downtime during deployments The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue.

The software engineers have decided to use AWS Codepipeline to manage their build and deployment process

Which solution will meet these requirements?

A.Use Github websockets to trigger the Codepipeline pipeline.Use the Jenkins plugin for AWSCodebuild to conduct unit testing.Send alerts to an Amazon SNS topic for any bad builds.Deploy inan in-place , all-at once deployment configuration using AWS Codedeploy

B.Use Github webhooks to trigger the Codepipeline pipeline.Use the Jenkins plugin for AWS Codebuild to conduct unit testing.Send alerts to an Amazon SNS topic for any bad builds Deploy in a blue/green deployment using AWS Codedeploy

C.Use Github websockets to trigger the Codepipeline pipeline Use AWS X-ray for unit testing and static code analysis.Send alerts to an Amazon SNS topic for any bad builds Deploy in a blue/greende ployment using AWS Codedeploy

D.Use Github webhooks to trigger the Codepieline pipeline Use AWS x Ray tor unit testing and static code analysis Sendalerts to an Amazon SNS topic for any bad builds. Deploy in an in place , ll-at- once deployment configuration using AWS Codedeploy

Answer: B

一家初创公司最近将一个大型电子商务网站迁移到了AWS该网站的销售额增长了70％

Sofware工程师正在使用私有的Github存储库来管理代码。devops团队正在使用Jenkins进行构建和单元测试。

工程师需要在部署期间收到有关不良构建和零停机时间的通知。工程师还需要确保对生产的任何更改对用户而言都是无缝的，并且在出现重大问题时可以回滚。

软件工程师已决定使用AWS Codepipeline来管理其构建和部署过程

哪种解决方案可以满足这些要求？

A.使用Github websockets触发Codepipeline管道;使用AWS Codebuild的Jenkins插件进行单元测试;针对任何不良构建，将警报发送到Amazon SNS主题。使用AWS Codedeploy进行就地，一次性部署配置

B.使用Github Webhooks触发Codepipeline管道。使用AWS Codebuild的Jenkins插件进行单元测试。将任何不良构建的警报发送到Amazon SNS主题使用AWS Codedeploy进行蓝色/绿色部署

C.使用Github websockets触发Codepipeline管道使用AWS X-ray进行单元测试和静态代码分析将警报发送到Amazon SNS主题以查找任何不良构建使用AWS Codedeploy以蓝色/绿色部署

D.使用Github webhooks触发Codepieline管道使用AWS x Ray Torr单元测试和静态代码分析Sendalerts到Amazon SNS主题以查找任何不良构建。使用AWS Codedeploy进行就地，一次性的部署配置

答案：B

Q40

A company has developed a mobile game.The backend for the game runs on several virtual machines located in an on-premises data center.

The business logic is exposed using a REST API with multiple functions.Player session data is stored in central file storage Backend services use different API keys for throttling and to distinguish between live and test traffic.

The load on the game backend vanes throughout the day.During peak hours the server capacity is not sufficient.

There are also latency issues when fetching player session data Management has asked a solutions architect to present a cloud architecture that can handle the games varying load and provide low- atency data access.The API model should not be changed

Which solution meets these requirements?

A.Implement the REST API using a Network Load Balancer(NLB ).Run the business logic on an Amazon EC2 instance behind the NLB.Store player session data in Amazon Aurora Serverless .

B.Implement the REST API using an Ap lication Load Balancer(ALB).Run the business logic in AWS Lambda Store player session data in Amazon Dynamodb with on demand capacity

C.Implement the REST API using Amazon API Gateway Run the business logic in AWS Lambda. Store player session data in Amazon Dynamodb with on-demand capacity.

D.Implement the REST API using AWS Appsync.Run the business logic in AWS Lambda.Store player session data in Amazon Aurora Serverless

Answer: C

一家公司开发了一款手机游戏，该游戏的后端运行在本地数据中心中的多个虚拟机上。

使用具有多种功能的REST API公开业务逻辑。播放器会话数据存储在中央文件存储中。后端服务使用不同的API密钥进行节流并区分实时流量和测试流量。

游戏后端的负载全天都在消散。在高峰时段，服务器容量不足。

在获取玩家会话数据时，还存在延迟问题。管理层要求解决方案架构师提供一种云体系结构，该云体系结构可以处理游戏中不同的负载并提供低效率的数据访问。不应更改API模型

哪种解决方案满足这些要求？

A.使用网络负载平衡器（NLB）实施REST API。在NLB后面的Amazon EC2实例上运行业务逻辑。将播放器会话数据存储在Amazon Aurora Serverless中。

B.使用授权负载均衡器（ALB）实施REST API。在AWS Lambda中以随需应变的容量在Amazon Dynamodb中存储播放器会话数据中的业务逻辑

C.使用Amazon API Gateway实施REST API,AWS Lambda中运行业务逻辑.按需容量在Amazon Dynamodb中存储播放器会话数据。

D。使用AWS Appsync实施REST API。在AWS Lambda中运行业务逻辑。在Amazon Aurora Serverless中存储播放器会话数据

Q41 **11/19考试原题**

A company hosts an application on Amazon EC2 instances and needs to store files in Amazon S3.The files should never traverse the public internet, and only the application EC2 instances are granted access to a specific Amazon S3 bucket A solutions architect has created a VPC endpoint for Amazon S3 and connected the endpoint to the application VPC .

Which additional steps should the solutions architect take to meet these requirements?

A.Assign an endpoint policy to the endpoint that restricts access to a specific S3 bucket Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint Add the gateway prefix list to a NACL of the instances to limit access to the application EC2 instances only

B.Attach a bucket policy to the S3 bucket that grants access to application EC2 instances only using the aws:Source condition.Update the VPC route table so only the application EC2 instances can access the VPC endpoint

C.Assign an endpoint policy to the VPC endpoint that restricts access to a specific S3 bucket.Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint.Assign an LAM role to the application EC2 instances and only allow access to the role in the S3 buckets policy. Attach a bucket policy to the VPC endpoint that restricts access to S3 in the current Region

D.Assign an endpoint policy to the VPC endpoint that restricts access to S3 in the current Region.Attach a bucket policy to the S3 bucket that grants access to the VPC the application EC2 instances only.Add the gateway prefix list to a NACL to limit access to the application EC2 instances only

Answer: C

一家公司在Amazon EC2实例上托管一个应用程序，需要将文件存储在Amazon S3中。这些文件永远不应遍历公共互联网，并且仅向该应用程序EC2实例授予对特定Amazon S3存储桶的访问权限解决方案架构师已创建了VPC终端节点用于Amazon S3并将端点连接到应用程序VPC。

解决方案架构师应采取哪些其他步骤来满足这些要求？

A.将端点策略分配给限制对特定S3存储桶访问的端点将存储桶策略附加到授予对VPC端点访问权限的S3存储桶将网关前缀列表添加到实例的NACL以限制对应用程序EC2的访问仅实例

B.将桶策略附加到仅使用aws：Source条件授予对应用程序EC2实例的访问权限的S3桶中。更新VPC路由表，以便仅应用程序EC2实例可以访问VPC端点

C.将端点策略分配给限制对特定S3存储桶访问的VPC端点;将存储桶策略分配给授予对VPC端点访问权限的S3存储桶;将LAM角色分配给应用程序EC2实例，并且仅允许访问S3存储桶策略中的角色。将存储桶策略附加到VPC终结点，以限制对当前区域中S3的访问

D.将端点策略分配给限制对当前区域中S3的访问的VPC端点;将存储桶策略附加到仅向应用程序EC2实例授予对VPC的访问权的S3存储桶;将网关前缀列表添加到NACL以限制仅访问应用程序EC2实例

Q42

A company is migrating its three-tier web application from on-premises to the AWS Cloud.The company has the following requirements for the migration process:

-Ingest machine Images from the on-prermises environment.

-Synchronize changes from the on-promises environment to the AWS environment until the production cutover.

-Minimize downtime when executing the Production Cutover

-Migrate the virtual machines root volumes and data volumes

which solution will satisfy these requirements with minimal operational overhead?

A.Use AWS Server Migration Service(SMS)to create and launch a replication job tor each tier of the application Launch instances from the AMIs created by AWS SMS After initial testing , perform a final replication and create new instances from the updated AMIs.

B.Create an AWS CLI VM Import/Export script to migrate each virtual machine Schedule the script to run incrementally to maintain changes in the application Launch instances from the AMIs created by VM Import/Export.Once testing is done , rerun the script to do a final import and launch the instances from the AMIs

C.Use AWS Server Migration Service(SMS)to upload the operating system volumes.Use the AWS CLI import-snapshot command for the data volumes.Launch instances from the AMIs created by AWS

SMS and attach the data volumes to the instances.After initial testing , perform a final replication .launch new instances from the replicated AMIs , and attach the data volumes to the instances

D.Use AWS Application Discovery Service and AWS Migration Hub to group the virtual machines as an application.Use the AWS CLI VM Import/Export script to import the virtural machines as AMIs. Schedule the script to run incrementally to maintain changes in the application Launch instances from the AMls.After initial testing perform a final virtual machine import and launch new instances from the AMIs

Answer：A

一家公司正在将其三层Web应用程序从本地迁移到AWS Cloud，该公司对迁移过程有以下要求：

-从本地环境中摄取机器镜像。

-同步从本地环境到AWS环境的更改，直到生产切换为止。

-最小化执行生产转换时的停机时间

-迁移虚拟机的根卷和数据卷

哪种解决方案将以最小的运营开销满足这些要求？

A.使用AWS Server Migration Service（SMS）创建和启动复制作业，以遍及应用程序的每一层。从AWS SMS创建的AMI启动实例。进行初始测试后，执行最终复制并从更新的AMI创建新实例。

B.创建一个AWS CLI VM导入/导出脚本以迁移每个虚拟机安排脚本以递增方式运行以维护应用程序中的更改从VM导入/导出创建的AMI启动实例。一旦测试完成，请重新运行该脚本最终导入并从AMI启动实例

C.使用AWS Server Migration Service（SMS）上载操作系统卷。对数据卷使用AWS CLI import-snapshot命令。从AWS创建的AMI启动实例

SMS并将数据卷附加到实例。进行初始测试后，执行最终复制。从复制的AMI启动新实例，然后将数据卷附加到实例

D.使用AWS Application Discovery Service和AWS Migration Hub将虚拟机作为应用程序进行分组。使用AWS CLI VM Import / Export脚本将虚拟机作为AMI导入。计划脚本以增量方式运行以维护应用程序中的更改从AMls启动实例。在初始测试之后，执行最终的虚拟机导入并从AMI启动新实例。

Q43.

A Company has an application that sells tickets Online and experiences bursts of demand every 7 days.The application has a stateless presentation layer running on Amazon EC2 , an Oracle database to store unstructured data catalog Information , and a backend API layer.The front-end layer uses an Elastic Load Balancer to distribute the load across nine On-demand Instances over three Availability Zones(AZs ).The Oracle database is running on a Single EC2 Instance.

The company is experiencing performance issues when running more than two Concurrent campaigns. A Solutions architect must design a solution that meets the following requirements

-Address Scalability Issues

-Increase the level of concurrency

-Eliminate licensing costs Im prove reliability

Which set of steps should the solutions architect take?

Create an Auto Scaling group for the front end with a combination of On-demand and Spot Instances to reduce costs Convert the Oracle database into a single Amazon RDS reserved DB instance

Create an Auto caling group for the front end with a combination of On-demand and Spotin stances to reduce costs Create two additional copies of the database instance , then distribute the databases in separate AZs

Create an Auto Scaling group for the front end with a combination of On-demand and Spot instances to reduce costs.Convert the tables in the Oracle database into Amazon Dynamodb tables

D.Convert the On-demand Instances into Spot Instances to reduce costs for the front end. Convert the tables in the Oracle database into Amazon Dynamodb tables

Answer:C

某公司有一个应用程序，该应用程序可以在线销售门票，每7天就会遇到大量需求。该应用程序具有在Amazon EC2上运行的无状态表示层，用于存储非结构化数据目录信息的Oracle数据库以及一个后端API层。层使用Elastic Load Balancer在三个可用区（AZ）上的9个按需实例之间分配负载。Oracle数据库在单个EC2实例上运行。

该公司在运行两个以上的并行广告系列时遇到性能问题。解决方案架构师必须设计满足以下要求的解决方案

-地址可伸缩性问题

-增加并发级别

-消除许可成本即时证明可靠性

解决方案架构师应采取哪些步骤？

A.通过按需实例和竞价型实例的组合为前端创建Auto Scaling组，以降低成本将Oracle数据库转换为单个Amazon RDS保留的数据库实例

B.通过按需和Spotin两种方式创建前端的自动校准组，以降低成本创建数据库实例的两个其他副本，然后将数据库分布在单独的可用区中

C.使用按需实例和竞价型实例的组合为前端创建一个Auto Scaling组，以降低成本将Oracle数据库中的表转换为Amazon Dynamodb表

D.将按需实例转换为竞价型实例以降低前端成本。将Oracle数据库中的表转换为Amazon Dynamodb表

答：C

Q44.

A developer reports receiving an Error 403:Access Denied message when they try to download an object from an Amazon S3 bucket.

The S3 bucket is accessed using an S3 endpoint inside a VPC,and is encrypted with an AWS KMS key .A solutions architect has verified that the developer is assuming the correct IAM role in the account that allows the object to be downloaded.The S3 bucket policy and the NACL are also valid Which additional step should the solutions architect take to troubleshoot this issue?

Ensure that blocking all public access has not been enabled in the S3 bucket

Verity that the IAM role has permission to decrypt the referenced KMS key

Verify that the IAM role has the correct trust relationship configured

Check that local firewall rules are not preventing access to the s3 endpoint

Answer: B

Q44。

开发人员报告说，他们尝试从Amazon S3存储桶下载对象时收到错误403：Access Denied消息。

使用VPC内的S3终结点访问S3存储桶，并使用AWS KMS密钥对其进行加密。解决方案架构师已验证开发人员在允许下载对象的账户中承担了正确的IAM角色。 策略和NACL也是有效的解决方案架构师应采取哪些其他步骤来解决此问题？

A.确保未在S3存储桶中启用阻止所有公共访问

B.证明IAM角色有权解密引用的KMS密钥

C.验证IAM角色是否配置了正确的信任关系

D.检查本地防火墙规则是否阻止访问s3端点

答案：B

Q45

A company is deploying a public-facing global application on AWS using Amazon Cloudfront.The application communicates with an external system. A solutions architect needs to ensure the data is secured during end-to-end transit and at rest.

Which combination of steps will satisfy these requirements?(Select THREE )

Create a public certificate for the required domain in AWS Certificate Manager and deploy it to Cloudfront, an Application Load Balancer, and Amazon EC2 instances

Acquire a public certificate from a third-party vendor and deploy it to Cloudfront, an ApplicaiionLoad Balancer and Amazon EC2 instances

Provision Amazon EBS encrypted volumes using AWS KMS and ensure explicit encryption of data when writing to Amazon EBS

D.Provision Amazon EBS encrypted volumes using AWS KMS

Use SSL or encrypt data while communicating with the external system using a VPN .

Communicate with the external system using plaintext and use the VPN to encrypt the data in transit

Answer: BDE

一家公司正在使用Amazon Cloudfront在AWS上部署面向公众的全局应用程序。该应用程序与外部系统进行通信。 解决方案架构师需要确保在端到端传输期间和静止时确保数据的安全。

哪些步骤组合可以满足这些要求？（选择3个）

A.在AWS Certificate Manager中为所需域创建一个公共证书，并将其部署到Cloudfront，Application Load Balancer和Amazon EC2实例

B.从第三方供应商获取公共证书，并将其部署到Cloudfront，ApplicaiionLoad Balancer和Amazon EC2实例

C.使用AWS KMS设置Amazon EBS加密卷并确保在写入Amazon EBS时对数据进行显式加密

D.使用AWS KMS设置Amazon EBS加密卷

E.在使用VPN与外部系统通信时，使用SSL或加密数据。

F.使用纯文本与外部系统通信，并使用VPN加密传输中的数据

Q46

An enterprise companys data science team wants to provide a safe , cost-effective way to provide easy access to Amazon Sagemaker.The data scientists have limited AWS knowledge and need to be able to launch a Jupyter notebook instance.The notebook instance needs to have a preconfigured AWS KMS key to encrypt data at rest on the machine learning storage volume without exposing the complex setup requirements

Which approach will allow the company to set up a self-service mechanism for the data scientists to launch Jupyter notebooks in its.

AWS accounts with the LEAST amount of operational overhead?

Create a serverless front end using a static Amazon S3 website to allow the data scientists to request a Jupyter notebook instance by filling out a form.Use Amazon API Gateway to receivere quests from the S3 website and trigger a central AWS Lambda function to make an API call to Amazon SageMaker that will launch a notebook instance with a preconfigured KMS key for the data scientists. Then call back to the front-end website to display the URL to the notebook instance

Create an AWS Cloudformation template to launch a Jupyter notebook instance using the AWS:SageMakerc:Notebooklnstance resource type with a preconfigured KMS key.Add a user-friendly name to the Cloudformation template Display the URL to the notebook using the Outputs section Distribute the Cloudformation template to the data scientists using a shared Amazon S3 bucket

Create an AWS Cloudformation template to launch a Jupyter notebook instance using the AWS:SageMakerc:Notebooklnstance resource type with a preconfigured KMS key.Simplify the parameter names , such as the instance size , by mapping them to Small , Large , and X-large using the Mappings section in Cloudformation.Display the URL to the notebook using the Outputs section , then upload the template into an AWS Service Catalog product in the data scientists portfolio , and share it with thedata scientist's LAM role

D.Create an AWS CH script that the data scientists can run locally.Provide step by-step instructions about the parameters to be provided while executing the AWS CLI script to launch a Jupyter notebook with a preconfigured KMS key Distribute the CLI script to the data scientists using a shared AmazonS3 bucket

Answer: C

一个企业公司的数据科学团队希望提供一种安全，经济高效的方式来轻松访问Amazon Sagemaker。数据科学家对AWS的了解有限，需要能够启动Jupyter notebook实例。预配置的AWS KMS密钥可加密机器学习存储卷上的静态数据，而无需暴露复杂的设置要求

哪种方法将使该公司建立一种自助服务机制，供数据科学家在其内部启动Jupyter notebook。

AWS账户的运营费用最少吗？

A.使用静态Amazon S3网站创建无服务器前端，以允许数据科学家填写表格来请求Jupyternotebook实例。使用Amazon API Gateway接收来自S3网站的请求并触发中央AWS Lambda函数对Amazon SageMaker的API调用，它将启动一个notebook实例，并为数据科学家提供一个预配置的KMS密钥。然后回拨到前端网站以显示notebook实例的URL

B.创建一个AWS Cloudformation模板以使用带有预先配置的KMS密钥的AWS：SageMakerc：NotebookInstance资源类型启动Jupyter notebook实例。向Cloudformation模板添加一个用户友好名称，使用Outputs部分显示notebook的URL分发使用共享的Amazon S3存储桶向数据科学家提供Cloudformation模板

C.创建一个AWS Cloudformation模板以使用带有预先配置的KMS密钥的AWS：SageMakerc：NotebookInstance资源类型启动Jupyter notebook实例。通过将参数名称映射到Small，Large和X-来简化参数名称，例如实例大小使用Cloudformation中的Mappings部分进行配置。使用Outputs部分显示notebook的URL，然后将该模板上传到数据科学家产品组合中的AWS Service Catalog产品中，并与数据科学家的IAM角色共享

D.创建一个数据科学家可以在本地运行的AWS CH脚本。提供有关在执行AWS CLI脚本以使用预配置的KMS密钥启动Jupyternotebook时要提供的参数的逐步说明科学家使用共享的AmazonS3存储桶

Q47

An enterprise company is building an infrastructure services platform for its users. The company has the following requirements:

-Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services.

• Use a central account to manage the creation of infrastructure services.

-Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations.

-Provide the ability to enforce tags on any infrastructure that is started by users.

Which combination of actions using AWS services will meet these requirements? (Choose three.)

A. Develop infrastructure services using AWS Cloud Formation templates.

Add the templates to a central Amazon S3 bucket and add the-IAM roles or users that require access to the S3 bucket policy.

B. Develop infrastructure services using AWS Cloud Formation templates.

Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account.

Share these portfolios with the Organizations structure created for the company.

C. Allow user 1AM roles to have AWSCIoudFormationFullAccess and AmazonS3ReadOnlyAccess permissions.

Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.

D. Allow user 1AM roles to have ServiceCatalogEndUserAccess permissions only.

Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption assign users access and apply launch constraints.

E. Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company.

Apply the TagOption to AWS Service Catalog products or portfolios.

F. Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users.

Answer: BDE

一家企业公司正在为其用户构建基础结构服务平台。公司有以下要求：

-在启动AWS基础架构时为用户提供最低特权访问，以便用户无法置备未经批准的服务。

•使用中央帐户来管理基础结构服务的创建。

-提供将基础架构服务分发到AWS Organizations中的多个账户的功能。

-提供在用户启动的任何基础架构上强制执行标签的功能。

使用AWS服务的哪种操作组合可以满足这些要求？ （选择三个。）

A.使用AWS Cloud Formation模板开发基础架构服务。

将模板添加到中央Amazon S3存储桶，然后添加-IAM角色或需要访问S3存储桶策略的用户。

B.使用AWS Cloud Formation模板开发基础架构服务。

将每个模板作为AWS Service Catalog产品上传到在中央AWS账户中创建的投资组合。

与为公司创建的组织结构共享这些投资组合。

C.允许用户1AM角色具有AWSCIoudFormationFullAccess和AmazonS3ReadOnlyAccess权限。

在AWS账户根用户级别添加组织SCP，以拒绝除AWS CloudFormation和Amazon S3之外的所有服务。

D.允许用户1AM角色仅具有ServiceCatalogEndUserAccess权限。

使用自动化脚本将中央投资组合导入到本地AWS账户，复制TagOption分配用户访问权限并应用启动约束。

E.使用AWS Service Catalog TagOption库维护公司所需的标签列表。

将TagOption应用于AWS Service Catalog产品或产品组合。

F.使用AWS CloudFormation资源标签属性将标签强制应用到将为用户创建的任何CloudFormation模板。

Q48.

A media company has a static web application that is generated programmatically The company has a build pipeline that generates HTML content that is uploaded to an Amazon S3 bucket served by Amazon Cloudfront.The build pipeline runs inside a Build Account.The S3 bucket and CloudFront distribution are in a Distibution Account.The build pipeline uploads the files to Amazon S3 using an 1AM role in the Build Account.The S3 bucket has a bucket policy that only allows CloudFront to read objects using an origin access identity (CAI).During testing , all attempts to access the application using the Cloudfront URL result in an HTTP 403 Access Denied response

What should a solutions architect suggest to the company to allow access the objects in Amazon S3 through Cloudfront?

Modify the S3 upload process in the Build Account to add the bucket-owner-full-control AOL to the objects at upload

Create a new cross-account AM role in the Distribution Account with write access to the 83 bucket Modify the buiid pipeline to assume this role to upload the files to the Distribution Account

Modify the S3 upload process in the Build Account to set the object owner to the Distribution Account

Create a new 1AM role in the Distribution Account with read access to the S3 bucket.Configure Cloudftont to use this new role as its OAL.Modify the build pipeline to assume this role when uploading files from the Build Account

Answer: D

一家媒体公司拥有以编程方式生成的静态Web应用程序该公司拥有一个生成管道，该生成管道生成HTML内容，该HTML内容上载到Amazon Cloudfront服务的Amazon S3存储桶中。该构建管道在Build Account中运行.S3存储桶和CloudFront发行版位于Distibution帐户中。构建管道使用构建帐户中的1AM角色将文件上传到Amazon S3.S3存储桶具有存储桶策略，该策略仅允许CloudFront使用源访问身份（CAI）读取对象。所有尝试使用Cloudfront URL访问应用程序的操作都会导致HTTP 403访问被拒绝响应

解决方案架构师应向公司建议什么，以允许通过Cloudfront访问Amazon S3中的对象？

A.修改构建帐户中的S3上传过程，将存储桶拥有者完全控制AOL添加到上传对象中

B.在具有对S3存储桶的写访问权的分发帐户中创建一个新的跨帐户IAM角色修改buiid管道以承担该角色，以将文件上传到分发帐户

C.修改构建帐户中的S3上传过程，以将对象所有者设置为分发帐户

D.在分发帐户中创建一个新的IAM角色，对S3存储桶具有读取访问权限。配置Cloudftont将此新角色用作其OAL。修改构建管道以在从构建帐户上传文件时承担此角色

Q49

A Solutions architect is implementing Infrastructure as code for a two-tier web application in an AWS Cloudformation template.The web frontend application will be deployed on Amazon EC2 instances in an Auto Scaling group.The backend database will be an Amazon RDS for MYSQL DB Instance.The database password will be rotated every 60 days

How can the solutions architect MOST securely manage the configuration of the applications database credentials?

Provide the database password as a parameter in the Cloudformation template.Create an initialization script in the Auto Scaling group s launch configuration Userdata property to reference to password parameter using the Ref intrinsic function Store the password on the EC2 instances Reference the parameter for the value of the MasterUserPassword property in the AWS RDS::Blnstance resource using the Ref intrinsic function

Create a new AWS Secrets Manager secret resource in the Cloudformation template to be used as the database password.Configure the application to retrieve the password from Secrets Manage when needed. Reference the secret resource for the value of the MasterUserPassword property in the AWS RDS::DBInstance resource using a dynamic reference

Create a new AWS Secrets Manager secret resource in the Cloudformation template to be used as the database password. Create an initialization script in the Auto Scaling groups launch configuration Userdata property to reference the secret resource using the Ref intrinsic function.Reference the secret resource for the value of the MasterUserPassword property in the AWS RDS:DNinstance resource using the Ref intrinsic function.

Create a new AWS Systems Manager Parameter Store parameter in the Cloudformation template to be used as the database password.Create an initialization script in the Auto Scaling group s launch configuration serdata property to reference the parameter Reference the parameter for the value of the MasterUserPassword property an the AWS RDS::DBinstance resource using the Fn::Ge Att intrinsic function

Answer: B

解决方案架构师正在AWS Cloudformation模板中将基础架构实现为两层Web应用程序的代码.Web前端应用程序将部署在Auto Scaling组中的Amazon EC2实例上。后端数据库将是适用于MYSQL DB实例的Amazon RDS,数据库密码每60天轮换一次

解决方案架构师如何才能MOST安全地管理应用程序数据库凭据的配置？

A.在Cloudformation模板中提供数据库密码作为参数。在Auto Scaling组的启动配置Userdata属性中创建一个初始化脚本，以使用Ref内在函数引用密码参数将密码存储在EC2实例上为该参数引用参数使用Ref内部函数的AWS RDS :: Blnstance资源中MasterUserPassword属性的值

B.在Cloudformation模板中创建一个新的AWS Secrets Manager秘密资源以用作数据库密码。配置应用程序以在需要时从Secrets Manage检索密码。请参考AWS RDS中MasterUserPassword属性值的秘密资源： ：DBInstance资源使用动态引用

C.在Cloudformation模板中创建一个新的AWS Secrets Manager机密资源以用作数据库密码。在Auto Scaling组启动配置Userdata属性中创建一个初始化脚本，以使用Ref内在函数引用该机密资源。使用Ref内部函数的AWS RDS：DNinstance资源中MasterUserPassword属性的值

D.在Cloudformation模板中创建一个新的AWS Systems Manager参数存储参数以用作数据库密码。在Auto Scaling组的启动配置serdata属性中创建一个初始化脚本，以引用该参数为MasterUserPassword的值引用该参数使用Fn :: Ge Att内在函数对AWS RDS :: DBinstance资源进行属性设置

答案：B

Q50

A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region The weather maps are updated frequently and stored in Amazon S3 along with static HTML content.The web application is fronted by Amazon Cloudfront:

The company recently expanded to serve users in the us-east-1 Region , and these new users report that viewing their respective weather maps is slow from time to time

Which combination of steps will resolve the us-east-1 performance issues?(Select TWO)

Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1 .Configure endpoint groups for TCP ports 80 and 443 in us-east-1

Create a new S3 bucket in us-east-1. Configure S3 cross-region replication to synchronize from the S3 bucket in eu-west-1

Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1.

Use Lambda@Edge to modify requests from North America to use the S3 bucket in us east-1.

Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the Cloudfront distribution. Use Lambda@Edge to modify requests from North America to use the new origin. Answer: BD

气象服务通过eu-west-1区域内AWS托管的Web应用程序提供高分辨率气象图。气象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开头：

该公司最近扩展了服务范围，以为us-east-1地区的用户提供服务，这些新用户报告说，查看其各自的天气地图有时会很慢

哪个步骤组合可以解决us-east-1的性能问题？（选择两个）

A.在eu-west-1中为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

B.在us-east-1中创建一个新的S3存储桶。配置S3跨区域复制以从eu-west-1中的S3存储桶同步

C.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。

D.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。

E.将us-east-1的AWS Global Accelerator端点配置为Cloudfront发行版上的来源。使用Lambda @ Edge修改来自北美的请求以使用新来源。

Q51

A company is using AWS CloudFormation as its deployment tool for all application. It stages all application binaries and templates within Amazon S3 bucket with versioning enable Developers have access to an Amazon EC2 instance that hosts the integrated development (IDE). The Developers download the application binaries from Amazon S3 to the EC2 instance, make changes, and upload the binaries to an S3 bucket after running the unit locally. The developers

want to improve the existing deployment mechanism and implement CI/CD using AWS CodePipeline.

The developers have the following requirements:

-Use AWS CodeCommit for source control.

Automate unit testing and security scanning.

-Alert the Developers when unit tests fail.

-Turn application features on and off, and customize deployment dynamically as part of CI/CD.

Have the lead Developer provide approval before deploying an application.

Which solution will meet these requirements?

A.Use AWS Code Build to run unit tests and security scans Use an Amazon Eventbridge rule to sendAmazon SNS alerts to the developers when unit tests fail. Write AWS Cloud Development Kit(AWS CDK) constructs for different solution features and use a manifest file to turn features on and off in the AWS CDK application: Use a manual approval stage in the pipeline to allow the lead developer to approve applications

B Use AWS Lambda to run unit tests and security scans Use Lambda in a subsequent stage in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Amplify plugins for different solution features and utilize user prompts to turn features on and off. Use Amazon SES in the pipeline to allow the lead developer to approve applications.

C Use Jenkins to run unit tests and security scans Use an Amazon Eventbridge rule in the pipeline to send Amazon SES alerts to the developers when unit tests fail. Use AWS Cloudformation nested stacks for different solution features and parameters to turn features on and off. Use AWS Lambda in the pipeline to allow the lead developer to approve applications

D.Use AWS Code Deploy to run unit tests and security scans Use an Amazon Cloudwatch alarm in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Use Docker images for different solution features and the AWS CLI to turn features on and off Use a manual approval stage in the pipeline to allow the lead developer to approve applications

Answer: A

一家公司正在使用AWS CloudFormation作为所有应用程序的部署工具。它通过版本控制对Amazon S3存储桶中的所有应用程序二进制文件和模板进行分段，使开发人员可以访问托管集成开发（IDE）的Amazon EC2实例。开发人员在本地运行单元后，将应用程序二进制文件从Amazon S3下载到EC2实例，进行更改，然后将二进制文件上传到S3存储桶。开发商

希望改善现有部署机制并使用AWS CodePipeline实施CI / CD。

开发人员具有以下要求：

-使用AWS CodeCommit进行源代码控制。

・自动化单元测试和安全扫描。

-当单元测试失败时提醒开发人员。

-打开和关闭应用程序功能，并作为CI / CD的一部分动态自定义部署。

・在部署应用程序之前，请首席开发人员提供批准。

哪种解决方案可以满足这些要求？

A.使用AWS Code Build运行单元测试和安全性扫描当单元测试失败时，使用Amazon Eventbridge规则将Amazon SNS警报发送给开发人员。编写适用于不同解决方案功能的AWS Cloud Development Kit（AWS CDK）构造并使用清单文件来打开和关闭AWS CDK应用程序中的功能：在管道中使用手动批准阶段，以允许潜在开发人员批准应用程序

B使用AWS Lambda运行单元测试和安全扫描，在单元测试失败时，在管道的后续阶段使用Lambda将Amazon SNS警报发送给开发人员。编写适用于不同解决方案功能的AWS Amplify插件，并利用用户提示打开和关闭功能。在管道中使用Amazon SES，以允许主要开发人员批准应用程序。

C使用Jenkins运行单元测试和安全扫描，在单元测试失败时，在管道中使用Amazon Eventbridge规则向开发人员发送Amazon SES警报。将AWS Cloudformation嵌套堆栈用于不同的解决方案功能和参数，以打开或关闭功能。在管道中使用AWS Lambda，以允许潜在开发人员批准应用程序

D.使用AWS Code Deploy运行单元测试和安全性扫描当单元测试失败时，在管道中使用Amazon Cloudwatch警报将Amazon SNS警报发送给开发人员。将Docker映像用于不同的解决方案功能，并使用AWS CLI打开和关闭功能。在管道中使用手动批准阶段以允许潜在开发人员批准应用程序

Q52

An ecommerce website running on AWS uses an Amazon RDS for MySQL DB instance with General Purpose SSD storage. The developers chose an appropriate instance type based on demand, and configured 100 GB of storage with a sufficient amount of free space.

The website was running smoothly for a few weeks until a marketing campaign launched. On the second day of the campaign, users reported long wait times and time outs. Amazon CloudWatch metrics indicated that both reads and writes to the DB instance were experiencing long response times. The CloudWatch metrics show 40% to 50% CPU and memory utilization, and sufficient free storage space is still available. The application server logs show no evidence of database connectivity issues.

What could be the root cause of the issue with the marketing campaign?

It exhausted the I/O credit balance due to provisioning low disk storage during the setup phase.

It caused the data in the tables to change frequently, requiring indexes to be rebuilt to optimize queries.

It exhausted the maximum number of allowed connections to the database instance.

It exhausted the network bandwidth available to the RDS for MySQL DB instance.

Answer: A

在AWS上运行的电子商务网站将Amazon RDS用于具有通用SSD存储的MySQL数据库实例。开发人员根据需求选择合适的实例类型，并配置100 GB的存储空间和足够的可用空间。

该网站运行了好几个星期，直到启动了营销活动。在广告系列的第二天，用户报告了漫长的等待时间和超时。 Amazon CloudWatch指标表明，对数据库实例的读写都经历了较长的响应时间。 CloudWatch指标显示40％到50％的CPU和内存利用率，并且仍然有足够的可用存储空间。应用程序服务器日志没有显示数据库连接问题的证据。

营销活动问题的根本原因是什么？

A由于在设置阶段配置了低磁盘存储，因此耗尽了I / O信用余额。

B.这导致表中的数据频繁更改，需要重建索引以优化查询。

C.它用尽了到数据库实例的最大允许连接数。

D.它耗尽了RDS for MySQL数据库实例可用的网络带宽。

Q53

A company built an ecommerce website on AWS using a three tier web architecture.The application Is Java based and composed of an Amazon Cloudfront distribution , an Apache web server layer of Amazon EC2 instances in an Auto Scaling group , and a backend Amazon Aurora MYSQL database.Last month , during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts.The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics.Some of the web servers were terminated before logs could be collected, and the Aurora metrics were not sufficient for query performance analysis .

Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events?(Select THREE )

Configure the Aurora MYSQL DB cluster to publish slow query and error logs to Amazon Cloudwatch Logs

Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2i nstances and implement tracing of SQL queries with the X Ray SDK for Java

Configure the Aurora MYSQL DB cluster to stream slow query and error logs to Amazon Kinesis □.Install and configure an Amazon Cloudwatch Logs agent on the EC2 instances to send the Apache logs to Cloudwatch Logs

Enable and configure AWS Cloudtrail to collect and analyze application activity from Amazon EC2 and Aurora

Enable Aurora MYSQL DB cluster performance benchmarking and publish the stream to AWS X-ray Answer: ABD

一家公司使用三层Web架构在AWS上构建了一个电子商务网站，该应用程序基于Java，由Amazon Cloudfront发行版，Auto Scaling组中的Amazon EC2实例的Apache Web服务器层以及后端Amazon Aurora MYSQL数据库组成上个月，在促销活动中，用户在向购物车添加商品时报告了错误和超时。操作团队恢复了由Web服务器创建的日志并审查了Aurora DB集群性能指标。可以收集日志，而Aurora指标不足以进行查询性能分析。

解决方案架构师必须采取哪些步骤组合来提高高峰流量事件期间应用程序性能的可见性？（选择3个）

A.配置Aurora MYSQL数据库集群以将慢速查询和错误日志发布到Amazon Cloudwatch Logs

B.实施AWS X-Ray SDK以在EC2i实例上跟踪传入的HTTP请求并使用X Ray SDK for Java实现对SQL查询的跟踪

C.配置Aurora MYSQL数据库集群以将缓慢的查询和错误日志流式传输到Amazon Kinesis

D.在EC2实例上安装并配置Amazon Cloudwatch Logs代理以将Apache日志发送到Cloudwatch Logs

E.启用并配置AWS Cloudtrail以收集和分析来自Amazon EC2和Aurora的应用程序活动

F启用Aurora MYSQL DB群集性能基准测试并将流发布到AWS X-ray

Q54

A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region.The application should dynamically scale to meet user demand and maintain resiliency.Additionally , the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region

Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

Create a VPC in the us-west-1 Region Use inter.Region VPC peering to connect both VPCs .Deploy an Application Load Balancer(ALB) spanning multiple Availability Zones(AZs)to the VPC in the us- east-1 Region Deploy EC2 instances across multiple AZs in each Region as part of an AutoScaling group spanning both VPCs and served by the ALB

Deploy an Application Load Baiancer(ALB) spanning multiple Availability Zones(AZs)to the VPC in the us-east-1 Region .Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region.Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions

Create a VPC in the us-west-1 Region.Use inter-region VPC peering to connect both VPCsDeploy an Application Load Balancer(ALB) that spans both VPCs.Deploy EC2 instances acrossmultiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB.Create an Amazon Route 53 record that points to the ALB

D.Deploy an Application Load Balancer(ALB) spanning multiple Availability Zones(AZs)to the VPC in the us east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB.Deploy the same solution to the us-west-1 Region.Create separate Amazon Route 53 records in each Region that point to the ALB in the Region.Use Route 53 health checks to provide high availability across both Regions

Answer: B

一家总部位于美国东海岸的北美公司正在us-east-1地区的Amazon EC2上运行新的Web应用程序，该应用程序应动态扩展以满足用户需求并保持弹性。此外，该应用程序必须具有灾难恢复功能us-west-1 Region在主动-被动配置中的功能

在us-east-1地区创建VPC之后，解决方案架构师应采取哪些步骤？

A.在us-west-1区域中创建VPC使用inter.Region VPC对等连接两个VPC。在us-east-1区域中的VPC部署跨越多个可用区（AZ）的应用程序负载均衡器（ALB） 。作为跨越两个VPC并由ALB服务的AutoScaling组的一部分，跨每个区域中的多个AZ部署EC2实例

B.将跨越多个可用区（AZ）的应用程序负载平衡器（ALB）部署到us-east-1地区中的VPC部署多个AZ中的EC2实例作为ALB服务的Auto Scaling组的一部分部署相同的解决方案us-west-1 Region。创建具有故障转移路由策略和运行状况检查的Amazon Route 53记录集，以在两个Region之间提供高可用性

C.在us-west-1区域中创建VPC。使用区域间VPC对等连接以连接两个VPC。部署跨两个VPC的应用程序负载平衡器（ALB）。跨多个可用区部署EC2实例作为Auto的一部分ALB服务的每个VPC中的扩展组。创建指向ALB的Amazon Route 53记录

D.将一个跨越多个可用区（AZ）的应用程序负载平衡器（ALB）部署到us-east-1地区中的VPC作为ECB部署的Auto Scaling组的一部分跨多个AZ部署EC2实例到us-west-1区域。在每个区域中创建指向该区域中ALB的单独Amazon Route 53记录。使用Route 53运行状况检查在两个区域中提供高可用性

Q55

A company has a web application that uses Amazon API Gateway , AWS Lambda , and Amazon Dynamodb.A recent marketing campaign has increased demand.Monitoring software reports thatmany requests have significantly longer response times than before the marketing campaign.A solutions architect enabled Amazon Cloudwatch Logs for API Gateway and noticed that errors are occurring on 20% of the requests

In Cloudwatch , the Lambda function Throttles metric represents 1% of the requests and the Errors metric represents 10% of the requests.Application logs indicate that, when errors occur, there is a call to Dynamodb

What change should the solutions architect make to improve the current response times as the web application becomes more popular?

lncrease the concurrency limit of the Lambda function

Implement Dynamodb auto scaling on the table

Increase the API Gateway throttle limit

Re-create the Dynamodb table with a better-partitioned primary index .

Answer: B

一家公司拥有一个使用Amazon API Gateway，AWS Lambda和Amazon Dynamodb的Web应用程序。最近的营销活动需求增加。监控软件报告许多请求的响应时间比营销活动之前明显更长。解决方案设计师启用了Amazon Cloudwatch Logs API Gateway，并注意到错误发生在20％的请求上

在Cloudwatch中，Lambda函数Throttles指标代表请求的1％，Errors指标代表请求的10％。应用程序日志表明，当发生错误时，有一个Dynamodb调用。

随着Web应用程序变得越来越流行，解决方案架构师应该进行哪些更改以改善当前响应时间？

A.增加Lambda函数的并发限制

B.在表上实施Dynamodb自动缩放

C.增加API网关的限制

D.重新创建具有更好分区的主索引的Dynamodb表。

Q56

A European online newspaper service hosts its public-facing Wordpress site in a colocated data center in London.The current Wordpress infrastructure consists of a load balancer;

TWO web servers , and one MYSQL database server.

A solutions architect is tasked with designing a solution with the following requirements:

-Improve the website s performance.

-Make the web tier scalable and stateless.

-Improve the database server performance for read-heavy loads

-Reduce latency for users across Europe and the US

・ Design the new architecture with a goal of 99.9 % availability.

Which solution meets these requirements while optimizing operational efficiency?

Use an Application Load Balancer(ALB) in front of an Auto Scaling group of Word press Amazon EC2 instances in one AWS Region and three Availability Zones.Configure an Amazon Elasticache cluster in front of Multi-az Amazon Aurora MYSQL DB cluster.Move the Wordpress shared files to Amazon EFS Configure Amazon Cioudfront with the ALB as the origin , and select a price class that includes the US and Europe

Use an Application Load Baiancer(ALB) in front of an Auto Scaling group of Word press Amazon EC2 instances in two AWS Regions and two Availability Zones in each Region.Configure an Amazon Elasticache cluster in front of a global Amazon Aurora MYSQL database.Move the Wordpress shared files to Amazon EFS.Configure Amazon Cloudfront with the ALB as the origin , and select a price class that includes the US and Europe.Configure EFS Cross Region replication

Use an Application Load Balancer(ALB) in front of an Auto Scaling group of Wordpress Amazon EC2 instances in one AWS Region and three Availability Zones.Configure an Amazon Documentdb table in front of a Multi-az Amazon Aurora MYSQL DB cluster.Move the Wordpress shared files to Amazon EFS.Configure Amazon Cloudfront with the ALB as the origin , and select a price class that includes all global locations

Use an Application Load Balancer(ALB) in front of an Auto Scaling group of Wordpress AmazonE2 instances in two AWS Regions and three Availability Zones in each Region.Configure an Amazon Elasticache cluster in front of a global Amazon Aurora MYSQL database.Move the Word press shared files to Amazon Fsx with cross-region synchronization.Configure Amazon Cloudfront with the ALB as the origin and a price class that includes the US and Europe

Answer: A

欧洲的一家在线报纸服务将其面向公众的Wordpress网站托管在伦敦的一个托管数据中心中。

两台Web服务器和一台MYSQL数据库服务器。

解决方案架构师的任务是设计具有以下要求的解决方案：

-提高网站的性能。

-使Web层可扩展且无状态。

-提高数据库服务器的性能，以应对重载

-减少欧洲和美国用户的延迟

・设计新架构，目标是99.9％的可用性。

在优化运营效率的同时，哪种解决方案可以满足这些要求？

A.在一个AWS区域和三个可用区中的Word press Amazon EC2实例的Auto Scaling组前面使用应用程序负载平衡器（ALB）。在Multi-az Amazon Aurora MYSQL DB群集前面配置Amazon Elasticache群集。将Wordpress共享文件传输到Amazon EFS以ALB为起点配置Amazon Cioudfront，然后选择一个包含美国和欧洲的价格类别

B.在两个AWS区域和每个区域的两个可用区中的Word press Amazon EC2实例的Auto Scaling组前面使用应用程序负载平衡器（ALB），在全局Amazon Aurora MYSQL数据库之前配置Amazon Elasticache集群。将Wordpress共享文件移动到Amazon EFS。配置以ALB为源的Amazon Cloudfront，然后选择包含美国和欧洲的价格类别。配置EFS跨区域复制

C.在一个AWS区域和三个可用区中的Wordpress Amazon EC2实例的Auto Scaling组的前面使用应用程序负载平衡器（ALB）。在Multi-az Amazon Aurora MYSQL DB集群前面配置Amazon Documentdb表。将Wordpress共享文件传输到Amazon EFS。以ALB为源配置Amazon Cloudfront，然后选择一个包含所有全局位置的价格类别

D 在两个AWS区域和每个区域的三个可用区中的Wordpress AmazonE2实例的Auto Scaling组的前面使用应用程序负载平衡器（ALB）在全局Amazon Aurora MYSQL数据库之前配置Amazon Elasticache集群。跨区域同步将文件共享到Amazon Fsx。以ALB为原点并包括美国和欧洲的价格类别配置Amazon Cloudfront

Q57

A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on- premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal, access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.

Which items should the solutions architect check to ensure identity federation is properly configured? (Choose three.)

The 1AM user's permissions policy has allowed the use of SAML federation for that user.

The 1AM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.

Test users are not in the AWSFederatedUsers group in the company's IdR.

The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the 1AM role, and the SAML assertion from IdR.

The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.

The company's IdP defines SAML assertions that properly map users or groups in the company to 1AM roles with appropriate permissions.

Answer: ABD

解决方案架构师已与其公司的内部身份提供商（IdP）实施了SAML 2.0联合身份解决方案，以验证用户对AWS环境的访问。当解决方案架构师通过联合身份Web门户测试身份验证时，将授予对AWS环境的访问权限。但是，当测试用户尝试通过联合身份Web门户进行身份验证时，他们将无法访问AWS环境。

解决方案架构师应检查哪些项目以确保正确配置身份联盟？ （选择三个。）

A IAM用户的权限策略已允许对该用户使用SAML联盟。

B.为联盟用户或联盟组的信任策略创建的1AM角色已将SAML提供程序设置为主体。

C.Test用户不在公司IdR的AWSFederatedUsers组中。

D. Web门户使用SAML提供者的ARN，1AM角色的ARN和IdR的SAML断言调用AWS STS AssumeRoleWithSAML API。

E.可从AWS环境VPC访问本地IdP的DNS主机名。

F.公司的IdP定义了SAML断言，这些断言可以正确地将公司中的用户或组映射到具有适当权限的1AM角色。

Q58

A company wants to improve cost awareness for its Amazon EMR platform.The company has allocated budgets for each teams Amazon EMR usage : When a budgetary threshold is reached , a notification should be sent by email to the budget office distibution list.Teams should be able to view their EMR cluster expenses to date.A solutions architect needs to create a solution that ensures this olicy is proactively and centrally enforced in a multi-account environment

Which combination of steps should the solutions architect take to meet these requirements?(selectTWO )

Update the AWS Cloudformation template to include the AWS : Budgests Budget resource with the Notifications ithsubscribers property

Implement Amazon Cloudwatch dashboards for Amazon EMR usage

Create an EMR bootstrap action that runs at startup that calls the Cost Explorer API to set the budget on the cluster with the Getcostforecast and Notifications ithsubscribers actions

Create an AWS Service Catalog portfolio for each team.Add each teams Amazon EMR cluster as an AWS Cloudformation template to their Service Catalog portfolio as a Product

Create an Amazon Cloudwatch metric for billing.Create a custom alert when costs exceed the budgetary threshold

Answer: AD

一家公司希望提高其Amazon EMR平台的成本意识。该公司已为每个团队分配了Amazon EMR使用量的预算：达到预算阈值时，应通过电子邮件将通知发送到预算办公室的分配列表。解决方案架构师需要创建一个解决方案，以确保在多帐户环境中主动并集中实施此策略

解决方案架构师应采取哪些步骤组合才能满足这些要求？（selectTWO）

A.更新AWS Cloudformation模板以包括带有Notification ithsubscribers属性的AWS：Budgests Budget资源

B.实施Amazon Cloudwatch仪表板以使用Amazon EMR

C.创建一个在启动时运行的EMR引导操作，该操作调用Cost Explorer API来使用Getcostforecast和Notifications ithsubscribers操作设置群集上的预算

D.为每个团队创建一个AWS Service Catalog产品组合。将每个团队Amazon EMR集群作为AWS Cloudformation模板添加到其Service Catalog产品组合中作为产品

E.创建用于计费的Amazon Cloudwatch指标。当成本超过预算阈值时创建自定义警报

Q59

A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population.The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers.The data platform must meet the following requirements -Provide near-real-time analytics of the inbound genomic data.

-Ensure the data is flexible , parallel , and durable.

-Deliver results of processing to a data warehouse

Which strategy should a solutions architect use to meet these requirements?

Use Amazon Kinesis Data Firehose to collect the inbound sensor data , analyze the data with Kinesis clients and save the results to an Amazon RDS instance.

Use Amazon Kinesis Data Streams to collect the inbound sensor data , analyze the data with Kinesis clients and save e results to an Amazon Redshift cluster using Amazon EMR

Use Amazon S3 to collect the inbound device data , analyze the data from Amazon SQS with Kinesis ,and save the results to an Amazon Redshift cluster

Use an Amazon API Gateway to put requests into an Amazon SQS queue , analyze the data with an AWS Lambda function , and save the results to an Amazon Redshift cluster using Amazon EMR

Answer: B

一家公司正在开发一种基因报告设备，该设备将收集基因组信息以帮助研究人员收集来自不同人群的大量数据样本，该设备将每秒将8 KB的基因组数据推送到一个数据平台，该数据平台需要处理和分析数据平台必须满足以下要求

-提供入站基因组数据的近实时分析。

-确保数据灵活，并行和持久。

-将处理结果传递到数据仓库

解决方案架构师应使用哪种策略来满足这些要求？

A.使用Amazon Kinesis Data Firehose收集入站传感器数据，使用Kinesis客户端分析数据并将结果保存到Amazon RDS实例。

B.使用Amazon Kinesis Data Streams收集入站传感器数据，使用Kinesis客户端分析数据并将结果保存到使用Amazon EMR的Amazon Redshift集群

C.使用Amazon S3收集入站设备数据，使用Kinesis分析来自Amazon SQS的数据，并将结果保存到Amazon Redshift集群

D.使用Amazon API Gateway将请求放入Amazon SQS队列中，使用AWS Lambda函数分析数据，然后使用Amazon EMR将结果保存到Amazon Redshift集群

9.15 add 41Q, Answer need Check

QUESTION 1

A company is using AWS CodePipeline for the CI/CD of an application to an Amazon EC2 Auto Scaling group. All AWS resources are defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the CloudFormation templates have caused unplanned downtime.

How should a solutions architect improve the CI/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?

Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments.

Write test plans for a testing team to execute in a non-production environment before approving the change for production.

Implement automated testing using AWS CodeBuild in a test environment.

Use CloudFormation change sets to evaluate changes before deployment

Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed.

Use plugins for the integrated development environment (IDE) to check the templates for errors, and use the AWS CLI to validate that the templates are correct.

Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and execute a manual test plan before approving the change for production.

Use AWS CodeDeploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts.

Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected.

Answer: B

一家公司正在将AWS CodePipeline用于Amazon EC2 Auto Scaling组的应用程序的CI / CD。所有AWS资源都在AWS CloudFormation模板中定义。应用程序工件存储在Amazon S3存储桶中，并使用实例用户数据脚本部署到Auto Scaling组。随着应用程序变得越来越复杂，CloudFormation模板中最近的资源更改已导致计划外停机。

解决方案架构师应如何改善CI / CD流水线，以减少模板更改将导致停机的可能性？

答：适应部署脚本以在执行部署时检测并报告CloudFormation错误情况。

编写测试计划，供测试团队在批准生产变更之前在非生产环境中执行。

B.在测试环境中使用AWS CodeBuild实施自动化测试。

使用CloudFormation变更集评估部署之前的变更

使用AWS CodeDeploy来利用蓝色/绿色部署模式，以进行评估并根据需要还原更改。

C.使用用于集成开发环境（IDE）的插件检查模板中的错误，并使用AWS CLI验证模板是否正确。

调整部署代码以检查错误情况并生成错误通知。在批准生产变更之前，请部署到测试环境并执行手动测试计划。

D.使用带有CloudFormation的AWS CodeDeploy和蓝/绿部署模式来替换用户数据部署脚本。

让操作员登录正在运行的实例并通过手动测试计划以验证应用程序是否按预期运行。

QUESTION 2

A web application is hosted in a dedicated VPC that is connected to a company's on-premises data center over a Site-to-Site VPN connection. The application is accessible from the company network only. This is a temporary non-production application that is used during business hours. The workload is generally low with occasional surges.

The application has an Amazon Aurora MySQL provisioned database cluster on the backend.

The VPC has an internet gateway and a NAT gateways attached. The web servers are in private subnets in an Auto Scaling group behind an Elastic Load Balancer. The web servers also upload data to an Amazon S3 bucket through the internet.

A solutions architect needs to reduce operational costs and simplify the architecture.

Which strategy should the solutions architect use?

Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only.

Use 3-year scheduled Reserved Instances for the web server EC2 instances.

Detach the internet gateway and remove the NAT gateways from the VPC.

Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket.

Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only.

Detach the internet gateway and remove the NAT gateways from the VPC.

Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.

Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only.

Detach the internet gateway from the VPC, and use an Aurora Serverless database.

Set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.

Use 3-year scheduled Reserved Instances for the web server Amazon EC2 instances. Remove the NAT gateways from the VPC, and set up a VPC endpoint for the S3 bucket. Use Amazon CloudWatch and AWS Lambda to stop and start the Aurora DB cluster so it operates during business hours only.

Update the network routing and security rules and policies related to the changes.

Answer: B

Web应用程序托管在专用的VPC中，该VPC通过站点到站点VPN连接连接到公司的本地数据中心。该应用程序只能从公司网络访问。这是在工作时间内使用的临时非生产应用程序。通常情况下，工作量较低，有时还会激增。

该应用程序在后端具有一个Amazon Aurora MySQL预配置的数据库集群。

VPC具有连接的Internet网关和NAT网关。 Web服务器位于弹性负载均衡器后面的Auto Scaling组中的专用子网中。 Web服务器还通过互联网将数据上传到Amazon S3存储桶。

解决方案架构师需要降低运营成本并简化架构。

解决方案架构师应使用哪种策略？

A.查看Auto Scaling组设置，并确保指定了计划的操作以仅在工作时间内操作Amazon EC2实例。

对Web服务器EC2实例使用3年计划的预留实例。

分离Internet网关，然后从VPC中删除NAT网关。

使用Aurora Serverless数据库并为S3存储桶设置VPC端点。

B.检查Auto Scaling组设置，并确保已指定计划的操作以仅在工作时间内操作Amazon EC2实例。

分离Internet网关，然后从VPC中删除NAT网关。

使用Aurora Serverless数据库并为S3存储桶设置VPC端点，然后更新与更改相关的网络路由，安全规则和策略。

C.查看Auto Scaling组设置，并确保指定了计划的操作以仅在工作时间内操作Amazon EC2实例。

从VPC分离Internet网关，并使用Aurora Serverless数据库。

为S3存储桶设置VPC端点，然后更新与更改有关的网络路由，安全规则和策略。

D.为Web服务器Amazon EC2实例使用3年计划的预留实例。从VPC删除NAT网关，并为S3存储桶设置VPC端点。使用Amazon CloudWatch和AWS Lambda停止和启动Aurora数据库集群，使其仅在工作时间内运行。

更新与更改有关的网络路由和安全规则和策略。

QUESTION 3

A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.

Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Choose three.)

Ensure the HPC cluster is launched within a single Availability Zone.

Launch the EC2 instances and attach elastic network interfaces in multiples of four.

Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.

Ensure the clusters is launched across multiple Availability Zones

Replace Amazon EFS win multiple Amazon EBS volumes in a RAID array.

Replace Amazon EFS with Amazon FSx for Lustre.

Answer: ACF

一家公司在AWS中构建了一个高性能计算（HPC）集群，用于紧密耦合的工作负载，该工作负载生成大量存储在Amazon EFS中的共享文件。 当集群中的Amazon EC2实例数为100时，集群表现良好。但是，当公司将集群规模增加到1,000个EC2实例时，总体性能大大低于预期。

解决方案架构师应该选择哪些设计选择集合，以从HPC集群中获得最大性能？ （选择三个。）

A.确保HPC群集在单个可用区中启动。

B.启动EC2实例，并以四个的倍数附加弹性网络接口。

C.选择启用了Elastic Fabric适配器（EFA）的EC2实例类型。

D.确保跨多个可用区启动群集

E.替换Amazon EFS在RAID阵列中赢得多个Amazon EBS卷。

F.使用Amazon FSx for Lustre替换Amazon EFS。

QUESTION 4

A company build an application based on AWS Lambda deployed in an AWS CloudFormation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release.

Which solution will meet these requirements?

Create an alias for every new deployed version of the Lambda function.

Use the AWS CLI update-alias command with the routing-config parameter to distribute the load.

Deploy the application into a new CloudFormation stack.

Use an Amazon Route 53 weighted routing policy to distribute the load.

Create a version for every new deployed Lambda function. Use the AWS CLI update-function- configuration command with the routing-config parameter to distribute the load.

Configure AWS CodeDeploy and use CodeDeployDe伯ult.OneAtATime in the Deployment configuration to distribute the load.

Answer: A

一家公司基于部署在AWS CloudFormation堆栈中的AWS Lambda构建应用程序。 Web应用程序的最新生产版本引入了一个问题，该问题导致中断持续了几分钟。 解决方案架构师必须调整部署过程以支持Canary发布。

哪种解决方案可以满足这些要求？

A为Lambda函数的每个新部署版本创建别名。

结合使用AWS CLI update-alias命令和routing-config参数来分配负载。

B.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。

C.为每个新部署的Lambda函数创建一个版本。 结合使用AWS CLI update-function-configuration命令和routing-config参数来分配负载。

D.配置AWS CodeDeploy并在Deployment配置中使用CodeDeployDe伯ult.OneAtATime来分配负载。

QUESTION 5

A company runs a popular public-facing ecommerce website. Its user base is growing quickly from a local market to a national market. The website is hosted in an on-premises data center with web servers and a MySQL database. The company wants to migrate its workload to AWS. A solutions architect needs to create a solution to:

Improve security

-Improve reliability

Improve availability

Reduce latency

Reduce maintenance

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

Use Amazon EC2 instances in two Availability Zones for the web servers in an Auto Scaling group behind an Application Load Balancer.

Migrate the database to a Multi-AZ Amazon Aurora MySQL DB cluster.

Use Amazon EC2 instances in two Availability Zones to host a highly available MySQL database cluster.

Host static website content in Amazon S3. Use S3 Transfer Acceleration to reduce latency while serving webpages. Use AWS WAF to improve website security.

Host static website content in Amazon S3. Use Amazon CloudFront to reduce latency while serving webpages. Use AWS WAF to improve website security.

Migrate the database to a single-AZ Amazon RDS for MySQL DB instance.

Answer:ABE

一家公司经营着一个受欢迎的面向公众的电子商务网站。它的用户群正在从本地市场迅速增长到全国市场。该网站托管在具有Web服务器和MySQL数据库的本地数据中心中。该公司希望将其工作负载迁移到AWS。解决方案架构师需要创建解决方案以：

・提高安全性

-提高可靠性

・提高可用性

・减少延迟

・减少维护

解决方案架构师应采取哪些步骤组合来满足这些要求？ （选择三个。）

A.在两个应用程序区域中的Amazon Scaling组中的Web服务器上使用Amazon EC2实例。

B.将数据库迁移到多可用区Amazon Aurora MySQL数据库集群。

C.在两个可用区中使用Amazon EC2实例来托管一个高可用性的MySQL数据库集群。

D.在Amazon S3中托管静态网站内容。使用S3 Transfer Acceleration减少提供网页时的延迟。使用AWS WAF改善网站安全性。

E.在Amazon S3中托管静态网站内容。使用Amazon CloudFront减少提供网页时的延迟。使用AWS WAF改善网站安全性。

F.将数据库迁移到MySQL数据库实例的单可用区Amazon RDS。

QUESTION 6

A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances in the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region. The users in Europe are reporting slow performance for their image uploads.

How can a solutions architect improve the performance of the image upload process?

Redeploy the application to use S3 multipart uploads.

Create an Amazon CloudFront distribution and point to the application as a custom origin.

Configure the buckets to use S3 Transfer Acceleration.

Create an Auto Scaling group for the EC2 instances and create a scaling policy. Answer: C

一家公司提供艺术品拍卖服务，并在北美和欧洲拥有用户。 该公司将其应用程序托管在us-east-1 Region中的Amazon EC2实例中。 艺术家将其作品的照片作为大尺寸高分辨率图像文件从手机上传到在us-east-1 Region中创建的集中式Amazon S3存储桶。 欧洲的用户报告他们的图像上传性能下降。

解决方案架构师如何提高图像上传过程的性能？

A：重新部署应用程序以使用S3分段上传。

B.创建一个Amazon CloudFront发行版并指向该应用程序作为自定义来源。

C.配置存储桶以使用S3传输加速。

D为EC2实例创建Auto Scaling组并创建扩展策略

QUESTION 7

A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on-premises data center. The company expects the new release will be downloaded by users worldwide. The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location.

Which solutions will meet these requirements?

Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group.

Configure an FTP service on the EC2 instances.

Use an Application Load Balancer in front of the Auto Scaling group.

Publish the game download URL for users to download the package.

Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group.

Configure an FTP service on the EC2 instances.

Use an Application Load Balancer in front of the Auto Scaling group.

Publish the game download URL for users to download the package.

Configure Amazon Route 53 and an Amazon S3 bucket for website hosting.

Upload the game files to the S3 bucket.

Use Amazon CloudFront for the website.

Publish the game download URL for users to download the package.

Configure Amazon Route 53 and an Amazon S3 bucket for website hosting.

Upload the game files to the S3 bucket.

Set Requester Pays for the S3 bucket.

Publish the game download URL for users to download the package.

Answer: C

一家公司开发了流行视频游戏的新版本，并希望将其公开提供。新发行包的大小约为5 GB。该公司从本地数据中心中托管的基于Linux的，面向公众的FTP站点提供现有版本的下载。该公司预计新版本将被全球用户下载。该公司希望提供一种解决方案，无论用户身在何处，都能提供改进的下载性能和较低的传输成本。

哪些解决方案可以满足这些要求？

答：将游戏文件存储在Auto Scaling组内Amazon EC2实例上安装的Amazon EBS卷上。

在EC2实例上配置FTP服务。

在Auto Scaling组的前面使用Application Load Balancer。

发布游戏下载URL，以供用户下载程序包。

B.将游戏文件存储在Auto Scaling组内附加到Amazon EC2实例的Amazon EFS卷上。

在EC2实例上配置FTP服务。

在Auto Scaling组的前面使用Application Load Balancer。

发布游戏下载URL，以供用户下载程序包。

C.配置Amazon Route 53和Amazon S3存储桶以进行网站托管。

将游戏文件上传到S3存储桶。

将Amazon CloudFront用于网站。

发布游戏下载URL，以供用户下载程序包。

D.为网站托管配置Amazon Route 53和Amazon S3存储桶。

将游戏文件上传到S3存储桶。

设置S3存储桶的请求者付款。

发布游戏下载URL，以供用户下载程序包。

QUESTION 8

A new startup is running a serverless application using AWS Lambda as the primary source of compute. New versions of the application must be made available to a subset of users before deploying changes to all users. Developers should also have the ability to abort the deployment and have access to an easy rollback mechanism. A solutions architect decides to use AWS CodeDeploy changes when a new version is available.CodeDeploy changes when a new version is available.

Which CodeDeploy configuration should the solutions architect use?

A blue/green deployment

A linear deployment

A canary deployment

An all-at-once deployment

Answer: C

一家新的初创公司正在使用AWS Lambda作为计算的主要来源来运行无服务器应用程序。 在将更改部署到所有用户之前，必须使该应用程序的新版本对部分用户可用。 开发人员还应该能够中止部署并可以使用简单的回滚机制。 解决方案架构师决定在有新版本可用时使用AWS CodeDeploy更改。在有新版本可用时使用CodeDeploy更改。解决方案架构师应使用哪种CodeDeploy配置？

A.蓝/绿部署

B.线性部署

C.金丝雀部署

D.一次部署

QUESTION 9

A company has developed a custom tool used in its workflow that runs within a Docker container. The company must perform manual steps each time the container code is updated to make the container image available to new workflow executions. The company wants to automate this process to eliminate manual effort and ensure a new container image is generated every time the tool code is updated.

Which combination of actions should a solutions architect take to meet these requirements? (Choose three.)

Configure an Amazon ECR repository for the tool. Configure an AWS CodeCommit repository containing code for the tool being deployed to the container image in Amazon ECR.

Configure an AWS CodeDeploy application that triggers an application version update that pulls the latest tool container image from Amazon ECR, updates the container with code from the source AWS CodeCommit repository, and pushes the updated container image to Amazon ECR.

Configuration an AWS CodeBuild project that pulls the latest tool container image from Amazon ECR, updates the container with code from the source AWS CodeCommit repository, and pushes the updated container image to Amazon ECR.

Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeDeploy application update.

Configure an Amazon EventBridge rule that triggers on commits to the AWS CodeCommit repository for the tool. Configure the event to trigger an update to the tool container image in Amazon ECR. Push the updated container image to Amazon ECR.

Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeBuild build.

Answer: ACF

一家公司开发了在其工作流中使用的自定义工具，该工具可在Docker容器中运行。每次更新容器代码时，公司必须执行手动步骤，以使容器图像可用于新的工作流程执行。该公司希望使这一过程自动化，以消除手工工作，并确保每次更新工具代码时都生成新的容器映像。

解决方案架构师应采取哪种行动组合来满足这些要求？ （选择三个。）

答：为该工具配置一个Amazon ECR存储库。配置一个AWS CodeCommit存储库，其中包含用于将工具部署到Amazon ECR中的容器映像的代码。

B.配置一个AWS CodeDeploy应用程序，该应用程序触发一个应用程序版本更新，该应用程序版本更新从Amazon ECR中提取最新的工具容器映像，并使用源AWS CodeCommit存储库中的代码更新该容器，然后将更新后的容器映像推送到Amazon ECR。

C.配置一个AWS CodeBuild项目，该项目从Amazon ECR中提取最新的工具容器映像，并使用源AWS CodeCommit存储库中的代码更新容器，并将更新后的容器映像推送到Amazon ECR。

D.配置一个AWS CodePipeline管道，该管道从AWS CodeCommit存储库中获取工具代码并启动AWS CodeDeploy应用程序更新。

E.配置一个Amazon EventBridge规则，该规则在对该工具的AWS CodeCommit存储库的提交时触发。配置事件以触发对Amazon ECR中的工具容器映像的更新。将更新的容器映像推送到Amazon ECR。

F.配置一个AWS CodePipeline管道，该管道从AWS CodeCommit存储库中获取工具代码并启动AWS CodeBuild构建。

QUESTION 10

A company needs to create a centralized logging architecture for all of its AWS accounts. The architecture should provide near-real-time data analysis for all AWS CloudTrail logs and VPC Flow Logs across all AWS accounts. The company plans to use Amazon Elasticsearch Service (Amazon ES) to perform log analysis in the logging account.

Which strategy a solutions architect use to meet these requirements?

Configure CloudTrail and VPC Flow Logs in each AWS account to send data to a centralized Amazon S3 bucket in the logging account.

Create and AWS Lambda function to load data from the S3 bucket to Amazon ES in the logging account.

Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch account.

Configure a CloudWatch subscription filter in each AWS account to send data to Amazon Kinesis Data Firehouse in the logging account.

Load data from Kinesis Data Firehouse into Amazon ES in the logging account.

Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket in each AWS account.

Create an AWS Lambda function triggered by S3 events to copy the data to a centralized logging bucket.

Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account

Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch Logs in each AWS account.

Create AWS Lambda functions in each AWS accounts to subscribe to the log groups and stream the data to an Amazon S3 bucket in the logging account.

Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account

Answer: B

公司需要为其所有AWS账户创建集中式日志记录架构。该架构应为所有AWS账户中的所有AWS CloudTrail日志和VPC流日志提供近乎实时的数据分析。该公司计划使用Amazon Elasticsearch Service（Amazon ES）在日志帐户中执行日志分析。

解决方案架构师使用哪种策略来满足这些要求？

A.在每个AWS账户中配置CloudTrail和VPC流日志，以将数据发送到日志账户中的集中式Amazon S3存储桶。

创建和AWS Lambda功能可将数据从S3存储桶加载到日志记录帐户中的Amazon ES。

B.配置CloudTrail和VPC流日志以将数据发送到Amazon CloudWatch帐户中的日志组。

在每个AWS帐户中配置CloudWatch订阅过滤器，以将数据发送到日志记录帐户中的Amazon Kinesis Data Firehouse。

将Kinesis Data Firehouse中的数据从日志帐户加载到Amazon ES。

C.配置CloudTrail和VPC流日志以将数据发送到每个AWS账户中的单独Amazon S3存储桶。

创建由S3事件触发的AWS Lambda函数，以将数据复制到集中式日志存储桶。

创建另一个Lambda函数以将S3存储桶中的数据加载到日志记录帐户中的Amazon ES

D.配置CloudTrail和VPC流日志以将数据发送到每个AWS账户中Amazon CloudWatch Logs中的日志组。

在每个AWS账户中创建AWS Lambda函数以订阅日志组，并将数据流式传输到日志记录账户中的Amazon S3存储桶。

创建另一个Lambda函数以将S3存储桶中的数据加载到日志记录帐户中的Amazon ES

QUESTION 11

A company standardized its method of deploying applications to AWS using AWS CodePipeline and AWS Cloud Formation. The applications are in TypeScript and Python. The company has recently acquired another business that deploys applications to AWS using Python scripts. Developers from the newly acquired company are hesitant to move their applications under Cloud Formation because it would require that they learn a new domain-specific language and eliminate their access to language features, such as looping.How can the acquired applications quickly be brought up to deployment standards while addressing the developers' concerns?

Create Cloud Formation templates and re-use parts of the Python scripts as Instance user data. Use the AWS Cloud Development Kit (AWS CDK) to deploy the application using these templates. Incorporate the AWS CDK into CodePipeline and deploy the application to AWS using these templates.

Use a third-party resource provisioning engine inside AWS CodeBuild to standardize the deployment processes of the existing and acquired company.

Orchestrate the CodeBuild job using CodePipeline.

Standardize on AWS OpsWorks. Integrate OpsWorks with CodePipeline. Have the developers create Chef recipes to deploy their applications on AWS.

Define the AWS resources using TypeScript or Python.

Use the AWS Cloud Development Kit (AWS CDK) to create CloudFormation templates from the developers' code, and use the AWS CDK to create CloudFormation stacks.

Incorporate the AWS CDK as a CodeBuild job in CodePipeline.

Answer: D

一家公司使用AWS CodePipeline和AWS Cloud Formation标准化了将应用程序部署到AWS的方法。这些应用程序使用TypeScript和Python。该公司最近收购了另一家使用Python脚本将应用程序部署到AWS的业务。新收购的公司的开发人员不愿将其应用程序迁移到Cloud Formation下，因为这将要求他们学习一种新的领域特定语言，并消除对语言功能（例如循环）的访问。

在解决开发人员的问题时，如何快速将获得的应用程序提升到部署标准？

A.创建Cloud Formation模板，并将Python脚本的某些部分作为实例用户数据重用。使用AWS Cloud Development Kit（AWS CDK）来使用这些模板部署应用程序。将AWS CDK整合到CodePipeline中，然后使用这些模板将应用程序部署到AWS。

B.在AWS CodeBuild中使用第三方资源供应引擎来标准化现有和被收购公司的部署流程。

使用CodePipeline编排CodeBuild作业。

C.在AWS OpsWorks上进行标准化。将OpsWorks与CodePipeline集成。让开发人员创建Chef食谱以将其应用程序部署在AWS上。

D.使用TypeScript或Python定义AWS资源。

使用AWS Cloud Development Kit（AWS CDK）从开发人员的代码创建CloudFormation模板，并使用AWS CDK创建CloudFormation堆栈。

将AWS CDK作为CodeBuild作业合并到CodePipeline中。

QUESTION 12

A healthcare company runs a production workload on AWS that stores highly sensitive personal information. The security team mandates that, for auditing purposes, any AWS API action using AWS account root user credentials must automatically create a high-priority ticket in the company's ticketing system. The ticketing system has a monthly 3-hour maintenance window when no tickets can be created.

To meet security requirements, the company enabled AWS CloudTrail logs and wrote a scheduled AWS Lambda function that uses Amazon Athena to query API actions performed by the root user. The Lambda function submits any actions found to the ticketing system API. During a recent security audit, the security team discovered that several tickets were not created because the ticketing system was unavailable due to planned maintenance.

a recent security audit, the security team discovered that several tickets were not created because the ticketing system was unavailable due to planned maintenance.

Which combination of steps should a solutions architect take to ensure that the incidents are reported to the ticketing system even during planned maintenance? (Choose two.)

Create an Amazon SNS topic to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to invoke the Lambda function.

Create an Amazon SQS queue to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to publish to the SQS queue.

Modify the Lambda function to be triggered by messages published to an Amazon SNS topic. Update the existing application code to retry every 5 minutes if the ticketing system's API endpoint is unavailable.

Modify the Lambda function to be triggered when there are messages in the Amazon SQS queue and to return successfully when the ticketing system API has processed the request.

Create an Amazon EventBridge rule that triggers on all API events where the invoking user identity is root.

Configure the EventBridge rule to write the event to an Amazon SQS queue.

Answer: BD

一家医疗保健公司在存储高度敏感的个人信息的AWS上运行生产工作负载。安全团队要求出于审核目的，使用AWS账户根用户凭证的任何AWS API操作必须在公司的票证系统中自动创建高优先级票证。票务系统具有每月3小时的维护时段，这段时间无法创建票证。

为了满足安全性要求，该公司启用了AWS CloudTrail日志并编写了计划的AWS Lambda函数，该函数使用Amazon Athena查询根用户执行的API操作。 Lambda函数将找到的所有操作提交到票务系统API。在最近的安全审核中，安全团队发现未创建多个票证，这是因为计划内的维护导致票证系统不可用。解决方案架构师应采取哪些步骤组合以确保即使在计划的维护期间也将事件报告给票务系统？ （选择两个。）

A.创建将向其发布Amazon CloudWatch警报的Amazon SNS主题。配置CloudWatch警报以调用Lambda函数。

B.创建将向其发布Amazon CloudWatch警报的Amazon SQS队列。配置CloudWatch警报以发布到SQS队列。

C.修改Lambda函数，使其由发布到Amazon SNS主题的消息触发。如果售票系统的API端点不可用，请更新现有应用程序代码以每5分钟重试一次。

D.修改Lambda函数，使其在Amazon SQS队列中有消息时触发，并在票务系统API处理请求后成功返回。

E.创建一个Amazon EventBridge规则，该规则在调用用户身份为root的所有API事件上触发。

捕捉api调用事件应为CloudTrail。

配置EventBridge规则以将事件写入Amazon SQS队列。

QUESTION 13

A company is running a two-tier web-based application in an on-premises data center. The application user consists of a single server running a stateful application. The application connects to a PostgreSQL database running on a separate server. The application's user base is expected to grow significantly, so the company is migrating the application and database to AWS.

The solution will use Amazon Aurora PostgreSQL, Amazon EC2 Auto Scaling, and Elastic Load Balancing.

Which solution will provide a consistent user experience that will allow the application and database tiers to scale?

Enable Aurora Auto Scaling for Aurora Replicas.

Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

Enable Aurora Auto Scaling for Aurora writes.

Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled.

Enable Aurora Auto Scaling for Aurora Replicas.

Use an Application Load Balancer with the robin routing and sticky sessions enabled.

Enable Aurora Scaling for Aurora writers.

Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

Answer: C

一家公司正在本地数据中心中运行基于Web的两层应用程序。应用程序用户由运行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。预计该应用程序的用户基础将显着增长，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。

哪种解决方案可以提供一致的用户体验，从而可以扩展应用程序和数据库层？

A.为Aurora副本启用Aurora自动缩放。

NLB 不支持粘性会话

副本才有自动缩放

使用启用了最少请求路由算法和粘性会话的网络负载平衡器。

B.为Aurora写入启用Aurora Auto Scaling。

在启用了循环路由算法和粘性会话的情况下使用Application Load Balancer。

C.为Aurora副本启用Aurora自动缩放。

在启用robin路由和错误会话的情况下使用Application Load Balancer。

D.为Aurora作家启用Aurora Scaling。

使用启用了最少请求路由算法和粘性会话的网络负载平衡器。

QUESTION 14

A solutions architect is designing a network for a new cloud deployment. Each account will need autonomy to modify route tables and make changes. Centralized and controlled egress internet connectivity is also needed. The cloud footprint is expected to grow to thousands of AWS accounts.

Which architecture will meet these requirements?

A centralized transit VPC with a VPN connection to a standalone VPC in each account.

Outbound internet traffic will be controlled by firewall appliances.

A centralized shared VPC with a subnet for each account.

Outbound internet traffic will be controlled through a fleet of proxy servers.

A shared services VPC to host central assets to include a fleet of firewalls with a route to the internet.

Each spoke VPC will peer to the central VPC.

A shared transit gateway to which each VPC will be attached. Outbound internet access will route through a fleet of VPN-attached firewalls. Answer: A

解决方案架构师正在设计用于新云部署的网络。 每个帐户都需要自治权来修改路由表并进行更改。 还需要集中和受控的出口Internet连接。 预计云足迹将增长到数千个AWS账户。

哪种架构可以满足这些要求？

A.集中传输VPC，每个帐户中都有到独立VPC的VPN连接。

出站互联网流量将由防火墙设备控制。

B.一个集中共享的VPC，每个帐户都有一个子网。

出站互联网流量将通过一组代理服务器进行控制。

C.共享服务VPC，用于托管中央资产，其中包括带有通往Internet的路由的防火墙群。每个发言的VPC都将与中央VPC对等。

D.每个VPC都将连接到的共享传输网关。 出站互联网访问将通过一组VPN连接的防火墙进行路由。

QUESTION 15

A solutions architect needs to migrate 50 TB of NFS data to Amazon S3. The files are on several NFS file servers on corporate network. These are dense file systems containing tens of millions of small files. The system operators have configured the file interface on an AWS Snowball Edge device and are using a shell script to copy data.

Developers report that copying the data to the Snowball Edge device is very slow. The solutions architect suspects this may be related to the overhead of encrypting all the small files and transporting them over the network.

Which changes can be made to speed up the data transfer?

Cluster two Snowball Edge devices together to increase the throughput of the devices.

Change the solution to use the S3 Adapter instead of the file interface on the Snowball Edge device.

Increase the number of parallel copy jobs to increase the throughput of the Snowball Edge device.

Connect directly to the USB interface on the Snowball Edge device and copy the files locally.

Answer: B

解决方案架构师需要将50 TB的NFS数据迁移到Amazon S3。这些文件位于公司网络上的多个NFS文件服务器上。这些是包含数千万个小文件的密集文件系统。系统操作员已在AWS Snowball Edge设备上配置了文件界面，并正在使用Shell脚本复制数据。

开发人员报告说，将数据复制到Snowball Edge设备非常慢。解决方案架构师怀疑这可能与加密所有小文件并通过网络传输它们的开销有关。

可以进行哪些更改以加快数据传输速度？

A.将两个Snowball Edge设备聚集在一起以增加设备的吞吐量。

B.更改解决方案以使用S3适配器而不是Snowball Edge设备上的文件接口。

C.增加并行复制作业的数量以增加Snowball Edge设备的吞吐量。

D.直接连接到Snowball Edge设备上的USB接口，然后在本地复制文件。

QUESTION 16

A company hosts a blog post application on AWS using Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. The application currently does not use API keys to authorize requests. The API model is as follows:

GET/posts/[postid] to get post details

GET/users[userid] to get user details

GET/comments/[commentid] to get comments details

The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by marking the comments appears in real time. Which design should be used to reduce comment latency and improve user experience?

Use edge-optimized API with Amazon CloudFront to cache API responses.

Modify the blog application code to request GET comment[commented] every 10 seconds.

Use AWS AppSync and leverage WebSockets to deliver comments.

Change the concurrency limit of the Lambda functions to lower the API response time. Answer: C

一家公司使用Amazon API Gateway，Amazon DynamoDB和AWS Lambda在AWS上托管博客文章应用程序。 该应用程序当前不使用API密钥来授权请求。 API模型如下：

GET / posts / [postid]获取帖子详细信息

GET / users [userid]获取用户详细信息

GET / comments / [commentid]以获取评论详细信息

该公司已注意到用户正在积极地在评论部分中讨论主题，并且该公司希望通过标记实时出现的评论来增加用户参与度。 应该使用哪种设计来减少评论延迟并改善用户体验？

A.将边缘优化的API与Amazon CloudFront一起使用以缓存API响应。

B.修改博客应用程序代码，以每10秒请求GET注释。

C.使用AWS AppSync并利用WebSockets发表评论。

D.更改Lambda函数的并发限制以减少API响应时间。

QUESTION 17

An loT company has rolled out a fleet of sensors for monitoring temperatures in remote locations. Each device connects to AWS loT Core and sends a message 30 seconds, updating an Amazon DynamoDB table. A System Administrator users AWS loT to verify the devices are still sending messages to AWS loT Core: the database is not updating.

What should a Solutions Architect check to determine why the database is not being updated?

Verify the AWS loT Device Shadow service is subscribed to the appropriate topic and is executing the AWS Lambda function.

Verify that AWS loT monitoring shows that the appropriate AWS loT rules are being executed, and that the AWS loT rules are enabled with the correct rule actions.

Check the AWS loT Fleet indexing service and verify that the thing group has the appropriate IAM role to update DynamoDB.

Verify that AWS loT things are using MQTT instead of MQTT over WebSocket, then check that the provisioning has the appropriate policy attached.

Answer: B

一家物联网公司已经推出了一组传感器，用于监视偏远地区的温度。 每个设备都连接到AWS loT Core，并在30秒内发送一条消息，以更新Amazon DynamoDB表。 系统管理员用户使用AWS loT验证设备仍在向AWS loT Core发送消息：数据库未更新。

解决方案架构师应检查什么以确定为什么不更新数据库？

A.验证AWS loT Device Shadow服务是否已订阅适当的主题并正在执行AWS Lambda函数。

B.验证AWS loT监视是否显示了正在执行适当的AWS loT规则，并且已使用正确的规则操作启用了AWS loT规则。

C.检查AWS loT Fleet索引服务并确认事物组具有适当的IAM角色以更新DynamoDB。

D.确认AWS物联网正在使用MQTT而非WebSocket上的MQTT，然后检查配置是否附加了适当的策略。

QUESTION 18 **11/19考试原题?**

An enterprise company is using a multi-account AWS strategy. There are separate accounts for development staging and production workloads. To control costs and improve governance the following requirements have been defined:

• The company must be able to calculate the AWS costs for each project.

-The company must be able to calculate the AWS costs for each environment development staging and production.

-Commonly deployed IT services must be centrally managed.

-Business units can deploy pre-approved IT services only.

-Usage of AWS resources in the development account must be limited.

Which combination of actions should be taken to meet these requirements? (Choose three.)

Apply environment, cost center, and application name tags to all taggable resources.

Configure custom budgets and define thresholds using Cost Explorer.

Configure AWS Trusted Advisor to obtain weekly emails with cost-saving estimates.

Create a portfolio for each business unit and add products to the portfolios using AWS CloudFormation in AWS Service Catalog.

Configure a billing alarm in Amazon CloudWatch.

Configure SCPs in AWS Organizations to allow services available using AWS.

Answer: ABD

一家企业公司正在使用多账户AWS策略。开发阶段和生产工作负载有单独的帐户。为了控制成本和改善治理，定义了以下要求：

•公司必须能够计算每个项目的AWS成本。

-公司必须能够计算每个环境开发阶段和生产的AWS成本。

-必须对集中部署的常用IT服务进行集中管理。

-业务部门只能部署预先批准的IT服务。

-必须限制开发帐户中AWS资源的使用。

应该采取哪些行动组合才能满足这些要求？ （选择三个。）

A.将环境，成本中心和应用程序名称标签应用于所有可标记资源。

B.使用Cost Explorer配置自定义预算并定义阈值。

C.配置AWS Trusted Advisor，以获取具有节省成本估算值的每周电子邮件。

D.为每个业务部门创建投资组合，然后使用AWS Service Catalog中的AWS CloudFormation将产品添加到投资组合中。

E.在Amazon CloudWatch中配置账单警报。

F.在AWS Organizations中配置SCP以允许使用AWS提供服务。

QUESTION 19

A company is planning to migrate an existing high performance computing (HPE) solution to the AWS Cloud. The existing solution consists of a 12-node cluster running Linux with high speed interconnectivity developed on a single rack. A solutions architect needs to optimize the performance of the HPE cluster.

Which combination of steps will meet these requirements? (Choose two.)

Deploy instances across at least three Availability Zones.

Deploy Amazon EC2 instances in a placement group.

Use Amazon EC2 instances that support Elastic Fabric Adapter (EFA).

Use Amazon EC2 instances that support burstable performance.

Enable CPU hyperthreading.

Answer: BC

一家公司计划将现有的高性能计算（HPE）解决方案迁移到AWS云。 现有解决方案由一个运行Linux的12节点群集组成，该群集具有在单个机架上开发的高速互连功能。 解决方案架构师需要优化HPE集群的性能。

哪些步骤组合可以满足这些要求？ （选择两个。）

A.至少在三个可用区中部署实例。

B.在放置组中部署Amazon EC2实例。

C.使用支持Elastic Fabric适配器（EFA）的Amazon EC2实例。

D.使用支持突发性能的Amazon EC2实例。

E.启用CPU超线程。

QUESTION 20

A company hosts a game player-matching service on a public facing, physical, on-premises instance that all users are able to access over the internet. All traffic to the instance uses UDP. The company wants to migrate the service to AWS and provide a high level of security. A solutions architect needs to design a solution for the player-matching service using AWS. Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

Use a Network Load Balancer (NLB) in front of the player-matching instance.

Use a friendly DNS entry in Amazon Route 53 pointing to the NLB's Elastic IP address.

Use an Application Load Balancer (ALB) in front of the player-matching instance.

Use a friendly DNS entry in Amazon Route 53 pointing to the ALB's internet-facing fully qualified domain name (FQDN).

Define an AWS WAF rule to explicitly drop non-UDP traffic, and associate the rule with the load balancer.

Configure a network ACL rule to block all non-UDP traffic.

Associate the network ACL with the subnets that hold the load balancer instances.

Use Amazon CloudFront with an Elastic Load Balancer as an origin.

Enable AWS Shield Advanced on all public-facing resources.

Answer: ADF

公司在面向公众的，物理的本地实例上托管游戏者匹配服务，所有用户都可以通过Internet访问该实例。到实例的所有流量都使用UDP。该公司希望将服务迁移到AWS并提供高级别的安全性。解决方案架构师需要使用AWS为玩家匹配服务设计解决方案。解决方案架构师应采取哪些步骤组合来满足这些要求？ （选择三个。）

A.在玩家匹配实例的前面使用网络负载平衡器（NLB）。

在Amazon Route 53中使用友好的DNS条目指向NLB的弹性IP地址。

B.在玩家匹配实例的前面使用应用程序负载平衡器（ALB）。

在Amazon Route 53中使用友好的DNS条目，指向ALB面向互联网的完全限定域名（FQDN）。

C.定义一个AWS WAF规则以显式丢弃非UDP流量，并将该规则与负载均衡器关联。

D.配置网络ACL规则以阻止所有非UDP流量。

将网络ACL与保存负载均衡器实例的子网相关联。

E.将Amazon CloudFront与Elastic Load Balancer作为来源使用。

F.在所有面向公众的资源上启用AWS Shield Advanced。

QUESTION 21

A company has multiple AWS accounts and manages these accounts which AWS Organizations. A developer was given IAM user credentials to access AWS resources. The developer should have read- only access to all Amazon S3 buckets in the account. However, when the developer tries to access the S3 buckets from the console, they receive an access denied error message with no bucket listed.

A solution architect reviews the permissions and finds that the developer's IAM user is listed as having read-only access to all S3 buckets in the account.

Which additional steps should the solutions architect take to troubleshoot the issue? (Choose

two )

Check the bucket policies for all S3 buckets.

Check the ACLs for all S3 buckets.

Check the SCPs set at the organizational units (OUs).

Check for the permissions boundaries set for the IAM user.

Check if an appropriate IAM role is attached to the IAM user.

Answer: CD

一家公司拥有多个AWS账户，并管理这些AWS组织。 为开发人员提供了IAM用户凭证，以访问AWS资源。 开发人员应该对该帐户中的所有Amazon S3存储桶具有只读访问权限。 但是，当开发人员尝试从控制台访问S3存储桶时，他们会收到拒绝访问错误消息，其中未列出存储桶。

解决方案架构师查看了权限，发现开发人员的IAM用户被列为具有对该帐户中所有S3存储桶的只读访问权限。

解决方案架构师应采取哪些其他步骤来解决问题？ （选择

两个）

A.检查所有S3存储桶的存储桶策略。

B.检查所有S3存储桶的ACL。

C.检查在组织单位（OU）设置的SCP。

D.检查为IAM用户设置的权限边界。

E.检查适当的IAM角色是否已附加到IAM用户。

QUESTION 22

A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into delays of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging. Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS distances.

Which strategy should the solutions architect provide to meet these requirements?

Use Tag Editor to tag existing resources.

Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources.

Use an AWS Config rule to alert the finance team of untagged resources.

Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role.

Use Tag Editor to tag existing resources.

Create cost allocation tags to define the cost center and project ID.

Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.

Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources.

Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource.

Answer: C

一家大型公司最近遇到了Amazon RDS和Amazon DynamoDB成本意外增加的情况。该公司需要提高对AWS Billing and Cost Management延迟的可见性。有许多与AWS Organizations相关的账户，包括许多开发和生产账户。在整个组织中没有一致的标记策略，但是有一些准则要求使用具有一致标记的AWS CloudFormation部署所有基础架构。管理需要所有现有和将来的DynamoDB表和RDS距离的成本中心编号和项目ID编号。

解决方案架构师应提供哪种策略来满足这些要求？

A.使用标记编辑器标记现有资源。

创建成本分配标签以定义成本中心和项目ID，并允许标签24小时传播到现有资源。

B.使用AWS Config规则提醒财务团队未加标签的资源。

创建一个基于集中式AWS Lambda的解决方案，以使用跨账户角色每小时标记未标记的RDS数据库和DynamoDB资源。

C.使用标记编辑器标记现有资源。

创建成本分配标签以定义成本中心和项目ID。

使用SCP限制资源上没有成本中心和项目ID的资源创建。

D.创建成本分配标签以定义成本中心和项目ID，并允许标签24小时传播到现有资源。

更新现有的联合角色以限制特权以供应不包括成本中心和资源的项目ID的资源。

QUESTION 23

A company has an application that generates reports and stores them in an Amazon bucket Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

Which set of action will immediately remediate the security issue without impacting the application's normal workflow?

Create an AWS Lambda function that applies all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.

Review the AWS Trusted advisor bucket permissions check and implement the recommend actions.

Run a script that puts a Private ACL on all of the object in the bucket.

Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcis option to TRUE on the bucket.

Answer: D

公司拥有一个生成报告的应用程序，并将其存储在Amazon S3存储桶中。 当用户访问其报告时，该应用程序会生成一个签名的URL，以允许用户下载该报告。 该公司的安全团队发现这些文件是公开的，并且任何人都可以在不进行身份验证的情况下下载它们。 该公司已暂停生成新报告，直到问题解决。

哪组操作将立即纠正安全问题，而又不影响应用程序的正常工作流程？

A.创建一个AWS Lambda函数，该函数将所有策略应用于未经身份验证的用户。 创建一个计划的事件以调用Lambda函数。

B.查看AWS Trusted Advisor存储桶权限检查并实施建议的操作。

C.运行一个脚本，该脚本将专用ACL放在存储桶中的所有对象上。

D.使用Amazon S3中的阻止公共访问功能将存储桶上的IgnorePublicApis选项设置为TRUE。

QUESTION 24

A company hosts a legacy application that runs on an Amazon EC2 instance inside a VPC without internet access. Users access the application with a desktop program installed on their corporate laptops. Communication between the laptops and the VPC flows through AWS Direct Connect (DX). A new requirement states that all data in transit must be encrypted between users and the VPC.

Which strategy should a solutions architect use to maintain consistent network performance while meeting this new requirement?

Create a client VPN endpoint and configure the laptops to use an AWS client VPN to connect to the VPC over the internet.

Create a new public virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX public virtual interface.

Create a new Site-to-Site VPN that connects to the VPC over the internet.

Create a new private virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX private virtual interface.

Answer: B

一家公司托管了一个遗留应用程序，该遗留应用程序在VPC内的Amazon EC2实例上运行，而没有Internet访问。用户使用在公司便携式计算机上安装的桌面程序访问该应用程序。便携式计算机和VPC之间的通信通过AWS Direct Connect（DX）进行。一项新要求规定，必须在用户和VPC之间对所有传输中的数据进行加密。

解决方案架构师应使用哪种策略来维持一致的网络性能，同时满足这一新要求？

A.创建一个客户端VPN终端节点，然后将笔记本电脑配置为使用AWS客户端VPN通过互联网连接到VPC。

B.为现有的DX连接创建一个新的公共虚拟接口，并创建一个通过DX公共虚拟接口连接到VPC的新VPN。

C.创建一个新的站点到站点VPN，该VPN通过Internet连接到VPC。

D.为现有的DX连接创建一个新的专用虚拟接口，并创建一个通过DX专用虚拟接口连接到VPC的新VPN。

QUESTION 25

A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.

In each AWS account with a client an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.

Which combination of steps should a solutions architect take to resolve this issue? (Choose two.)

Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets.

Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances.

Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets.

Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances.

Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets.

Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the clients.

Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets.

Answer: A C

,r'-"

一家公司正在创建在Amazon EC2上运行的集中式日志记录服务，该服务将接收和分析来自数百个AWS账户的日志。 AWS PrivateLink用于提供客户端服务和日志记录服务之间的连接。

在具有客户端的每个AWS账户中，已为日志记录服务创建了接口终端节点，并且该终端节点可用。在EC2实例上运行的日志记录服务通过网络负载平衡器（NLB）部署在不同的子网中。客户端无法使用VPC端点提交日志。

解决方案架构师应采取哪些步骤组合来解决此问题？ （选择两个。）

A.检查NACL是否已连接到日志服务子网，以允许与NLB子网之间的通信。

检查NACL是否已连接到NLB子网以允许与EC2实例上运行的日志记录服务子网之间的通信。

B.检查NACL是否已连接到日志服务子网，以允许与接口端点子网之间的通信。

检查NACL是否已连接到接口终结点子网，以允许与EC2实例上运行的日志记录服务子网之间的通信。

C.检查在EC2实例上运行的日志记录服务的安全组，以确保它允许从NLB子网进入。

D.检查在EC2实例上运行的日志记录服务的安全组，以确保它允许从客户端进入。

E.检查NLB的安全组，以确保它允许从接口终结点子网进入。

QUESTION 26

A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:

High availability within an AWS Region

-Able to fail over in 1 minute to another AWS Region for disaster recovery

Provide the most efficient solution while minimizing the impact on the user experience

Which combination of steps will meet these requirements? (Choose three.)

Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live (TTL) to 1 hour.

Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.

Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.

Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3.

Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region.

Have a script import the data into DynamoDB in a disaster recovery scenario.

Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions.

Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.

Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions.

Use Spot Instances for the required resources.

Answer: BCD

解决方案架构师需要为具有Web，应用程序和NoSQL数据层的三层应用程序定义解决方案的参考体系结构。参考体系结构必须满足以下要求：

•AWS区域内的高可用性

-能够在1分钟内故障转移到另一个AWS区域以进行灾难恢复

•提供最有效的解决方案，同时最大程度地减少对用户体验的影响

哪些步骤组合可以满足这些要求？ （选择三个。）

A.在两个选定区域中使用设置为100/0的Amazon Route 53加权路由策略。将生存时间（TTL）设置为1小时。

B.将Amazon Route 53故障转移路由策略用于从主区域到灾难恢复区域的故障转移。将生存时间（TTL）设置为30秒。

C.在Amazon DynamoDB中使用全局表，以便可以在两个选定的区域中访问数据。

D.每60分钟从主区域中的Amazon DynamoDB表中备份数据，然后将数据写入Amazon S3。

使用S3跨区域复制将数据从主区域复制到灾难恢复区域。

在灾难恢复方案中，让脚本将数据导入DynamoDB。

使用Auto Scaling组为区域中多个可用区中的Web和应用程序层实施热备用模型。

将区域保留实例用于最少数量的服务器，将按需实例用于任何其他资源。

E.在区域中的多个可用区中为Web和应用程序层使用Auto Scaling组。

使用竞价型实例获取所需的资源。

QUESTION 27 **11/19考试原题**

A company runs an application on a fleet of Amazon EC2 instances. The application requires low latency and random access to 100 GB of data. The application must be able to access the data at up to 3.000 IOPS. A Development team has configured the EC2 launch template to provision a 100-GB Provisioned IOPS (PIOPS) Amazon EBS volume with 3 000 IOPS provisioned. A Solutions Architect is tasked with lowering costs without impacting performance and durability. Which action should be taken?

Create an Amazon EFS file system with the performance mode set to Max I/O.

Configure the EC2 operating system to mount the EFS file system.

Create an Amazon EFS file system with the throughput mode set to Provisioned.

Configure the EC2 operating system to mount the EFS file system.

Update the EC2 launch template to allocate a new 1-TB EBS General Purpose SSO (gp2) volume.

Update the EC2 launch template to exclude the PIOPS volume.

Configure the application to use local instance storage.

Answer: C

家公司在一系列Amazon EC2实例上运行应用程序。 该应用程序要求低延迟并可以随机访问100 GB的数据。 该应用程序必须能够以高达3,000 IOPS的速度访问数据。 一个开发团队已配置EC2启动模板，以配置100 GB的IOPS（PIOPS）Amazon EBS卷和3000 IOPS。 解决方案架构师的任务是在不影响性能和耐用性的前提下降低成本。 应该采取什么行动？

A.创建一个性能模式设置为“最大I / O”的Amazon EFS文件系统。

配置EC2操作系统以挂载EFS文件系统。

B.创建一个Amazon EFS文件系统，并将吞吐量模式设置为Provisioned。

配置EC2操作系统以挂载EFS文件系统。

C.更新EC2启动模板以分配新的1 TB EBS通用SSO（gp2）卷。

D.更新EC2启动模板以排除PIOPS卷。

配置应用程序以使用本地实例存储。

QUESTION 28

A company recently transformed its legacy infrastructure provisioning scripts to AWS CloudFormation templates. The newly developed templates are hosted in the company's private GitHub repository. Since adopting CloudFormation, the company has encountered several issues with updates to the CloudFormation templates, causing execution or creating environment. Management is concerned by the increase in errors and has asked a Solutions Architect to design the automated testing of CloudFormation template updates. What should the Solution Architect do to meet these requirements?

Use AWS CodePipeline to create a change set from the CloudFormation templates stored in the private GitHub repository.

Execute the change set using AWS CodeDeploy.

Include a CodePipeline action to test the deployment with testing scripts run by AWS CodeBuild.

Mirror the GitHub repository to AWS CodeCommit using AWS Lambda.

Use AWS CodeDeploy to create a change set from the CloudFormation templates and execute it. Have CodeDeploy test the deployment with testing scripts run by AWS CodeBuild.

Use AWS CodePipeline to create and execute a change set from the CloudFormation templates stored in the GitHub repository.

Configure a CodePipeline action to be deployment with testing scripts run by AWS CodeBuild.

Mirror the GitHub repository to AWS CodeCommit using AWS Lambda.Use AWS CodeBuild to create a change set from the CloudFormation templates and execute it. Have CodeBuild test the deployment with testing scripts.

Answer: C

一家公司最近将其旧版基础架构配置脚本转换为AWS CloudFormation模板。新开发的模板托管在公司的私有GitHub存储库中。自采用CloudFormation以来，该公司在CloudFormation模板的更新中遇到了多个问题，导致执行或创建环境。管理层对错误的增加感到担忧，并要求解决方案架构师设计CloudFormation模板更新的自动化测试。解决方案架构师应该怎么做才能满足这些要求？

A.使用AWS CodePipeline从存储在私有GitHub存储库中的CloudFormation模板创建更改集。

使用AWS CodeDeploy执行更改集。

包括CodePipeline操作以使用由AWS CodeBuild运行的测试脚本来测试部署。

B.使用AWS Lambda将GitHub存储库镜像到AWS CodeCommit。

使用AWS CodeDeploy从CloudFormation模板创建一个变更集并执行它。让CodeDeploy使用AWS CodeBuild运行的测试脚本来测试部署。

C.使用AWS CodePipeline从GitHub存储库中存储的CloudFormation模板创建并执行更改集。

将CodePipeline操作配置为使用AWS CodeBuild运行的测试脚本进行部署。

D.使用AWS Lambda将GitHub存储库镜像到AWS CodeCommit。使用AWS CodeBuild从CloudFormation模板创建一个变更集并执行它。让CodeBuild使用测试脚本测试部署。

QUESTION 29

A company wants to improve cost awareness for its Amazon EMR platform. The company has allocated budgets for each team's Amazon EMR usage. When a budgetary threshold is reached, a notification should be sent by email to the budget office's distribution list. Teams should be able to view their EMR cluster expenses to date. A solutions architect needs to create a solution that ensures the policy is proactively and centrally enforced in a multi-account environment.

Which combination of steps should the solutions architect take to meet these requirements?

(Choose two.)

Update the AWS CloudFormation template to include the AWS::Budgets::Budget::resource with the NotificationsWithSubscribers property.

Implement Amazon CloudWatch dashboards for Amazon EMR usage.

Create an EMR bootstrap action that runs at startup that calls the Cost Explorer API to set the budget on the cluster with the GetCostForecast and NotificationsWithSubscribers actions.

Create an AWS Service Catalog portfolio for each team.

Add each team's Amazon EMR cluster as an AWS CloudFormation template to their Service Catalog portfolio as a Product.

Create an Amazon CloudWatch metric for billing.

Create a custom alert when costs exceed the budgetary threshold.

Answer: AD

一家公司希望提高其Amazon EMR平台的成本意识。该公司已为每个团队的Amazon EMR使用量分配了预算。当达到预算阈值时，应通过电子邮件将通知发送到预算办公室的分发列表。团队迄今为止应该能够查看其EMR群集费用。解决方案架构师需要创建一个解决方案，以确保在多帐户环境中主动并集中实施该策略。

解决方案架构师应采取哪些步骤组合来满足这些要求？

（选择两个。）

A.更新AWS CloudFormation模板以将AWS :: Budgets :: Budget :: resource包含到NotificationsWithSubscribers属性中。

B.实施Amazon CloudWatch仪表板以使用Amazon EMR。

C.创建一个在启动时运行的EMR引导操作，该操作调用Cost Explorer API来使用GetCostForecast和NotificationsWithSubscribers操作在群集上设置预算。

D.为每个团队创建一个AWS Service Catalog产品组合。

将每个团队的Amazon EMR集群作为AWS CloudFormation模板添加到其服务目录产品组合作为产品。

E.创建一个Amazon CloudWatch指标进行计费。

当费用超过预算阈值时，创建自定义警报。

QUESTION 30

A company is migrating its on-premises systems to AWS. The user environment consists of the following systems:

-Windows and Linux virtual machines running on VMware.

-Physical servers running Red Hat Enterprise Linux.

The company wants to be able to perform the following steps before migrating to AWS:

-Identify dependencies between on-premises systems.

-Group systems together into applications to build migration plans.

-Review performance data using Amazon Athena to ensure that Amazon EC2 instances are right-sized.

How can these requirements be met?

Populate the AWS Application Discovery Service import template with information from an on­premises configuration management database (CMDB).

Upload the completed import template to Amazon S3, then import the data into Application Discovery Service.

Install the AWS Application Discovery Service Discovery Agent on each of the on-premises systems.

Allow the Discovery Agent to collect data for a period of time.

Install the AWS Application Discovery Service Discovery Connector on each of the on-premises systems and in VMware vCenter.

Allow the Discovery Connector to collect data for one week.

Install the AWS Application Discovery Service Discovery Agent on the physical on-pre-map servers.

install the AWS Application Discovery Service Discovery Connector in VMware vCenter.

Allow the Discovery Agent to collect data for a period of time.

Answer: D

一家公司正在将其本地系统迁移到AWS。用户环境由以下系统组成：

-在VMware上运行的Windows和Linux虚拟机。

-运行Red Hat Enterprise Linux的物理服务器。

该公司希望能够在迁移到AWS之前执行以下步骤：

-识别本地系统之间的依赖关系。

-将系统组合到应用程序中以构建迁移计划。

-使用Amazon Athena查看性能数据，以确保大小合适的Amazon EC2实例。

如何满足这些要求？

A.使用内部配置管理数据库（CMDB）的信息填充AWS Application Discovery服务导入模板。

将完成的导入模板上传到Amazon S3，然后将数据导入Application Discovery Service。

B.在每个本地系统上安装AWS Application Discovery Service发现代理。

允许发现代理收集一段时间的数据。

C.在每个本地系统和VMware vCenter中安装AWS Application Discovery Service发现连接器。

允许发现连接器收集一周的数据。

D.在物理预映射服务器上安装AWS Application Discovery Service发现代理。

在VMware vCenter中安装AWS Application Discovery Service发现连接器。

允许发现代理收集一段时间的数据。

QUESTION 31

A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in MYSQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west- 2, and has configured Amazon Route 53 health checks and DNS failover to us-west-2.

Which additional step should the solutions architect take?

Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us- west-2.

Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2.

Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment.

Create a MySQL standby database on an Amazon EC2 instance in us-west-2. Answer: A**→答案变更B**

一家公司在us-east-1地区的AWS上托管一个Web应用程序。应用程序服务器分布在应用程序负载平衡器后面的三个可用区中。该数据库托管在Amazon EC2实例上的MYSQL数据库中。解决方案架构师需要使用AWS服务设计跨区域数据恢复解决方案，其RTO少于5分钟，RPO少于1分钟。解决方案架构师正在us-west-2中部署应用程序服务器，并已配置Amazon Route 53运行状况检查和DNS故障转移到us-west-2。

解决方案架构师应该采取哪一步？

A.将数据库迁移到uswest-2中具有跨区域只读副本的Amazon RDS for MySQL实例。

B.将数据库迁移到Amazon Aurora全局数据库，其中主数据库位于us-east-1中，辅助数据库位于us-west-1中。

C.将数据库迁移到具有多可用区部署的Amazon RDS for MySQL实例。

D.在us-west-2中的Amazon EC2实例上创建MySQL备用数据库。

QUESTION 32

A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MYSQL, and Oracle databases. There are many department services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

Which tools or services should solutions architect use to plan the cloud migration (Choose three.)

AWS Application Discovery Service

AWS SMS

AWS x-Ray

AWS Cloud Adoption Readness Tool (CART)

Amazon Inspector

AWS Migration Hub

Answer: ABF **→ ADF**

一家公司希望将其本地数据中心迁移到AWS Cloud。 其中包括数千个虚拟化Linux和Microsoft Windows服务器，SAN存储，带有MYSQL的Java和PHP应用程序以及Oracle数据库。 在同一数据中心或外部托管有许多部门服务。 技术文档不完整且过时。 解决方案架构师需要了解当前环境，并在迁移后估算云资源成本。

解决方案架构师应使用哪些工具或服务来计划云迁移（选择三项）。

A.AWS Application Discovery Service

B.AWS SMS

C.AWS x-Ray

D.AWS Cloud Adoption Readness Tool (CART)

E.Amazon Inspector

F.AWS Migration Hub

QUESTION 33

A company decided to purchase Amazon EC2 Reserved Instances. A solutions architect is tasked with implementing a solution where only the master account in AWS Organizations is able to purchase the Reserved Instances. Current and future member accounts should be blocked from purchasing Reserved Instances.

Which solution will meet these requirements?

Create an SCP with the Deny effect on the ec2:PurchaseReservedlnstancesOffering action. Attach the SCP to the root of the organization.

Create a new organizational unit (OU) Move all current member accounts to the new OU. Create an SCP with the Deny effect on the ec2:PurchaseReservedlnstancesOffering action. Attach the SCP to the new OU.

Create an AWS Config rule event that triggers automation that will terminate any Reserved Instances launched by member accounts.

Create two new organizational units (OUs): OU1 and OU2.

Move all member accounts to OU2 and the master account to OU1.

Create an SCP with the Allow effect on the ec2:PurchaseReservedlnstancesOffering action. Attach the SCP to OU1.

Answer: B

一家公司决定购买Amazon EC2预留实例。解决方案架构师的任务是实施解决方案，其中只有AWS Organizations中的主账户才能购买预留实例。当前和将来的成员帐户应被禁止购买预留实例。

哪种解决方案可以满足这些要求？

A.创建一个对ec2：PurchaseReservedInstancesOffer动作具有拒绝作用的SCP。将SCP附加到组织的根目录。

B.创建一个新的组织单位（OU）将所有当前成员帐户移到新的OU。创建一个对ec2：PurchaseReservedInstancesOffering操作具有“拒绝”效果的SCP。将SCP附加到新的OU。

C.创建一个触发自动化的AWS Config规则事件，该事件将终止由成员账户启动的所有预留实例。

D.创建两个新的组织单位（OU）：OU1和OU2。

将所有成员帐户移动到OU2，将主帐户移动到OU1。

创建一个对ec2：PurchaseReservedInstancesOffering操作具有“允许”效果的SCP。将SCP附加到OU1。

QUESTION 34

A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.

What is the MOST cost-effective migration recommendation?

Create a queue using Amazon SQS.

Configure the existing web server to publish to the new queue.

When there are messages in the queue, invoke an AWS Lambda function to puii requests from the queue and process the files.

Store the processed files in an Amazon S3 bucket.

Create a queue using Amazon MQ.

Configure the existing web server to publish to the new queue.

When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files.

Store the processed files in Amazon EFS. Shut down the EC2 instance after the task is complete.

Create a queue using Amazon MQ.

Configure the existing web server to publish to the new queue.

When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files.

Store the processed files in Amazon EFS.

Create a queue using Amazon SQS.

Configure the existing web server to publish to the new queue.

Use Amazon EC2 instances in an EC2 Auto scaling group to pull requests from the queue and process the files.

Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket

Answer: D

解决方案架构师需要向公司提供有关如何将其本地数据处理应用程序迁移到AWS Cloud的建议。当前，用户通过Web门户上传输入文件。然后，Web服务器将上载的文件存储在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个小时来处理。该公司已确定，等待处理的媒体文件数量在工作时间内显着增加，而工作时间之后文件数量迅速下降。

MOST具有成本效益的迁移建议是什么？

A.使用Amazon SQS创建队列。

配置现有的Web服务器以发布到新队列。

当队列中有消息时，请调用AWS Lambda函数以处理来自队列的请求并处理文件。

将处理后的文件存储在Amazon S3存储桶中。

B.使用Amazon MQ创建队列。

配置现有的Web服务器以发布到新队列。

当队列中有消息时，请创建一个新的Amazon EC2实例以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。任务完成后，关闭EC2实例。

C.使用Amazon MQ创建队列。

配置现有的Web服务器以发布到新队列。

当队列中有消息时，请调用AWS Lambda函数以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。

D.使用Amazon SQS创建队列。

配置现有的Web服务器以发布到新队列。

在EC2自动扩展组中使用Amazon EC2实例从队列中拉出请求并处理文件。

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

QUESTION 35

A company has a media catalog with metadata for each item in the catalog. Different types of metadata are extracted from the media items by an application running on AWS Lambda. Metadata is extracted according to a number of rules with the output stored in an Amazon ElastiCache for Redis cluster. The extraction process is done in batches and takes around 40 minutes to complete.

The update process is triggered manually whenever the metadata extraction rules change.

The company wants to reduce the amount of time it takes to extract metadata from its media catalog. To achieve this, a solutions architect has split the single metadata extraction Lambda function into a Lambda function for each type of metadata.

Which additional steps should the solutions architect take to meet the requirements?

Create an AWS Step Functions workflow to run the Lambda functions in parallel.

Create another Step Functions workflow that retrieves a list of media items and executes a metadata extraction workflow for each one.

Create an AWS Batch compute environment for each Lambda function. Configure an AWS Batch job queue for the compute environment.

Create a Lambda function to retrieve a list of media items and write each item to the job queue.

C. Create an AWS Step Functions workflow to run the Lambda functions in parallel.

Create a Lambda function to retrieve a list of media items and write each item to an Amazon SQS

queue.

Configure the SQS queue as an input to the Step Functions workflow.

Create a Lambda function to retrieve a list of media items and write each item to an Amazon SQS queue.

Subscribe the metadata extraction Lambda functions to the SQS queue with a large batch size.

Answer: D

公司有一个媒体目录，其中包含目录中每个项目的元数据。 AWS Lambda上运行的应用程序从媒体项目中提取不同类型的元数据。根据许多规则提取元数据，并将输出存储在Amazon ElastiCache for Redis集群中。提取过程是分批完成的，大约需要40分钟才能完成。

每当元数据提取规则更改时，手动触发更新过程。

该公司希望减少从媒体目录中提取元数据所花费的时间。为了实现这一点，解决方案架构师已将每种元数据类型的单个元数据提取Lambda函数拆分为Lambda函数。

解决方案架构师应采取哪些其他步骤来满足要求？

A.创建一个AWS Step Functions工作流以并行运行Lambda函数。

创建另一个/ Step Functions工作流，以检索媒体项目列表并为每个项目执行元数据提取工作流。

B.为每个Lambda函数创建一个AWS Batch计算环境。为计算环境配置一个AWS Batch作业队列。

创建Lambda函数以检索媒体项目列表并将每个项目写入作业队列。

C.创建一个AWS Step Functions工作流以并行运行Lambda函数。

创建Lambda函数以检索媒体项目列表，并将每个项目写入Amazon SQS队列。

将SQS队列配置为/ Step Functions工作流程的输入。

D.创建Lambda函数以检索媒体项目列表，并将每个项目写入Amazon SQS队列。

将元数据提取Lambda函数订阅到具有大批处理大小的SQS队列。

QUESTION 36

An AWS partner company is building a service in AWS Organizations using its organization named org1. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account. What is the MOST secure way to allow org1 to access resources in org2?

The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks.

The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks.

The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) when requesting access to perform the required tasks.

The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN), including the external ID in the IAM role's trust policy, when requesting access to perform the required tasks. Answer: D

一个AWS合作伙伴公司正在使用其名为org1的组织在AWS Organizations中构建服务。此服务要求合作伙伴公司有权访问客户帐户中的AWS资源，该客户帐户位于名为org2的单独组织中。公司必须使用API​​或命令行工具对客户帐户建立最低特权安全访问。允许org1访问org2中的资源的最安全的方法是什么？

答：客户应向合作伙伴公司提供其AWS账户访问密钥，以登录并执行所需的任务。

B.客户应创建一个IAM用户，并将所需的权限分配给IAM用户。然后，客户应将凭据提供给合作伙伴公司以登录并执行所需的任务。

C.客户应创建一个IAM角色，并将所需的权限分配给IAM角色。然后，合作伙伴公司在请求访问权限以执行所需任务时，应使用IAM角色的Amazon资源名称（ARN）。

D.客户应创建一个IAM角色，并将所需的权限分配给IAM角色。然后，合作伙伴公司在请求访问权限以执行所需任务时，应使用IAM角色的Amazon资源名称（ARN），包括IAM角色的信任策略中的外部ID。

QUESTION 37

A company's security compliance requirements state that all Amazon EC2 images must be scanned for vulnerabilities and must pass a CVE assessment. A solutions architect is developing a mechanism to create security- approved AMIs that can be used by developers. Any new AMIs should go through an automated assessment process and be marked as approved before developers can use them. The approved images must be scanned every 30 days to ensure compliance.

Which combination of steps should the solutions architect take to meet these requirements while following best practices? (Choose two.)

Use the AWS Systems Manager EC2 agent to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.

Use AWS Lambda to write automatic approval rules.

Store the approved AMI list in AWS Systems Manager Parameter Store.

Use Amazon EventBridge to trigger an AWS Systems Manager Automation document on all EC2 instances every 30 days.

Use Amazon Inspector to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.

Use AWS Lambda to write automatic approval rules.

Store the approved AMI list in AWS Systems Manager Parameter Store.

Use a managed AWS Config rule for continuous scanning on all EC2 instances, and use AWS Systems Manager Automation documents for remediation.

Use AWS CloudTrail to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.

Answer: BC

公司的安全合规性要求规定，必须扫描所有Amazon EC2映像的漏洞，并且必须通过CVE评估。解决方案架构师正在开发一种机制，以创建可供开发人员使用的安全性认可的AMI。任何新的AMI都应经过自动评估过程，并标记为已批准，然后开发人员才能使用它们。批准的/图像必须每30天扫描一次，以确保符合规定。

在遵循最佳实践的同时，解决方案架构师应采取哪些步骤组合来满足这些要求？ （选择两个。）

A.使用AWS Systems Manager EC2代理对从需要扫描的AMI启动的EC2实例运行CVE评估。

B.使用AWS Lambda编写自动批准规则。

将批准的AMI列表存储在AWS Systems Manager参数存储中。

每30天使用Amazon EventBridge在所有EC2实例上触发一个AWS Systems Manager自动化文档。

C.使用Amazon Inspector对从需要扫描的AMI启动的EC2实例运行CVE评估。

D.使用AWS Lambda编写自动批准规则。

将批准的AMI列表存储在AWS Systems Manager参数存储中。

使用托管的AWS Config规则对所有EC2实例进行连续扫描，并使用AWS Systems Manager自动化文档进行修复。

E.使用AWS CloudTrail对从需要扫描的AMI启动的EC2实例运行CVE评估。

QUESTION 38

A company is launching a web-based application in multiple regions around the world. The application consists of both static content stored in a private Amazon S3 bucket and dynamic content hosted in Amazon ECS containers content behind an Application Load Balancer (ALB). The company requires that the static and dynamic application content be accessible through Amazon CloudFront only.

Which combination of steps should a solutions architect recommend to restrict direct content access to CloudFront? (Choose three.)

Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB.

Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the CloudFront distribution.

Configure CloudFront to add a custom header to origin requests.

Configure the ALB to add a custom header to HTTP requests.

Update the S3 bucket ACL to allow access from the CloudFront distribution only.

Create a CloudFront Origin Access Identity (OAI) and add it to the CloudFront distribution. Update the S3 bucket policy to allow access to the OAI only.

Answer: ACF

一家公司正在全球多个地区启动基于Web的应用程序。该应用程序由存储在私有Amazon S3存储桶中的静态内容和由Amazon ECS容器托管的动态内容组成，位于应用程序负载平衡器（ALB）后面。该公司要求只能通过Amazon CloudFront访问静态和动态应用程序内容。

解决方案架构师应建议哪种步骤组合来限制对CloudFront的直接内容访问？ （选择三个。）

A.在AWS WAF中使用规则创建Web ACL，以验证自定义标头的存在并将Web ACL与ALB关联。

B.在AWS WAF中使用规则创建Web ACL，以验证自定义标头的存在并将Web ACL与CloudFront分配相关联。

C.配置CloudFront以向自定义请求添加自定义标头。

D.配置ALB以向HTTP请求添加自定义标头。

E.更新S3存储桶ACL以仅允许从CloudFront发行版进行访问。

F.创建一个CloudFront原始访问身份（OAI）并将其添加到CloudFront分发中。更新S3存储桶策略以仅允许访问OAI。

QUESTION 39

A company has multiple lines of business (LOBs) that roll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements: -Produce a single AWS invoice for all of the AWS accounts used by its LOBs.

・ The costs for each LOB account should be broken out on the invoice.

-Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy.

-Each LOB account should be deiegated full administrator permissions, regardless of the governance policy.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

Use AWS Organizations to create an organization in the parent account for each LOB. Then, invite each LOB account to the appropriate organization.

Use AWS Organizations to create a single organization in the parent account.

Then, invite each LOB's AWS account to join the organization.

Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB as appropriate.

Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts.

E.Enable consolidated billing in the parent account's billing console and link the LOB accounts.

Answer: DE

一个公司有多个业务线（LOB），这些业务线汇总到母公司。该公司已要求其解决方案架构师开发具有以下要求的解决方案：

-为其LOB使用的所有AWS账户生成一个AWS发票。

・每个LOB帐户的费用应在发票上细分。

-根据公司的治理策略，提供限制LOB帐户中的服务和功能的功能。

-无论治理策略如何，每个LOB帐户都应被授予完全管理员权限。

解决方案架构师应采取哪些步骤组合来满足这些要求？ （选择两个。）

A.使用AWS Organizations在父账户中为每个LOB创建一个组织。然后，邀请每个LOB帐户到适当的组织。

B.使用AWS Organizations在父账户中创建一个组织。然后，邀请每个LOB的AWS帐户固定该组织。

C.实施服务配额以定义允许的服务和功能，并将配额适当地应用于每个LOB。

D.创建一个仅允许批准的服务和功能的SCP，然后将策略应用于LOB帐户。

E.在上级帐户的计费控制台中启用合并计费，并链接LOB帐户。

QUESTION 40

A solutions architect has been assigned to migrate a 50 TB Oracle data warehouse that contains sales data from on-premises to Amazon Redshift. Major updates to the sales data occur on the final calendar day of the month. For the remainder of the month, the data warehouse only receives minor daily updates and is primarily used for reading and reporting. Because of this, the migration process must start on the first day of the month and must be complete before the next set of updates occur. This provides approximately 30 days to complete the migration and ensure that the minor daily changes have been synchronized with the Amazon Redshift data warehouse. Because the migration cannot impact normal business network operations, the bandwidth allocated to the migration for moving data over the internet is 50 Mbps. The company wants to keep data migration costs low.

Which steps will allow the solutions architect to perform the migration within the specified timeline?

Install Oracle database software on an Amazon EC2 instance. Configure VPN connectivity between AWS and the company's data center. Configure the Oracle database running on Amazon EC2 to join the Oracle Real Application Clusters (RAC).

When the Oracle database on Amazon EC2 finishes synchronizing, create an AWS DMS ongoing replication task to migrate the data from the Oracle database on Amazon EC2 to Amazon Redshift. Verify the data migration is complete and perform the cut over to Amazon Redshift.

Create an AWS Snowball import job. Export a backup of the Oracle data warehouse. Copy the exported data to the Snowball device. Return the Snowball device to AWS. Create an Amazon RDS for Oracle database and restore the backup file to that RDS instance. Create an AWS DMS task to migrate the data from the RDS for Oracle database to Amazon Redshift.

Copy daily incremental backups from Oracle in the data center to the RDS for Oracle database over the internet.

Verify the data migration is complete and perform the cut over to Amazon Redshift.

Install Oracle database software on an Amazon EC2 instance.

To minimize the migration time, configure VPN connectivity between AWS and the company's data center by provisioning a 1 Gbps AWS Direct Connect connection.

Configure the Oracle database running on Amazon EC2 to be a read replica of the data center Oracle database. Start the synchronization process between the company's on-premises data center and the Oracle database on Amazon EC2.

When the Oracle database on Amazon EC2 is synchronized with the on-premises database, create an AWS DMS ongoing replication task to migrate the data from the Oracle database read replica that is running on Amazon EC2 to Amazon Redshift.

Verify the data migration is complete and perform the cut over to Amazon Redshift.

Create an AWS Snowball import job. Configure a server in the company's data center with an extraction agent.

Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schema.

Create a new project in AWS SCT using the registered data extraction agent.

Create a local task and an AWS DMS task in AWS SCT with replication of ongoing changes. Copy data to the Snowball device and return the Snowball device to AWS.

Allow AWS DMS to copy data from Amazon S3 to Amazon Redshift.

Verify that the data migration is complete and perform the cut over to Amazon Redshift.

Answer: D

已指派解决方案架构师将包含销售数据的50 TB Oracle数据仓库从本地迁移到Amazon Redshift。销售数据的主要更新发生在该月的最后一个日历日。在该月的剩余时间内，数据仓库仅收到次要的每日更新，并且主要用于读取和报告。因此，迁移过程必须在每月的第一天开始，并且必须在下一组更新发生之前完成。这提供了大约30天的时间来完成迁移，并确保每日的次要更改已与Amazon Redshift数据仓库同步。由于迁移不会影响正常的业务网络操作，因此分配给迁移以通过Internet移动数据的带宽为50 Mbps。该公司希望保持较低的数据迁移成本。

解决方案架构师可以通过哪些步骤在指定的时间范围内执行迁移？

A.在Amazon EC2实例上安装Oracle数据库软件。配置AWS与公司数据中心之间的VPN连接。将运行在Amazon EC2上的Oracle数据库配置为加入Oracle Real Application Clusters（RAC）。

当Amazon EC2上的Oracle数据库完成同步后，创建一个AWS DMS正在进行的复制任务，以将数据从Amazon EC2上的Oracle数据库迁移到Amazon Redshift。确认数据迁移已完成，然后执行到Amazon Redshift的切换。

B.创建一个AWS Snowball导入作业。导出Oracle数据仓库的备份。将导出的数据复制到Snowball设备。将Snowball设备返回到AWS。为Amazon数据库创建Amazon RDS，然后将备份文件还原到该RDS实例。创建一个AWS DMS任务以将数据从RDS for Oracle数据库迁移到Amazon Redshift。

将每日增量备份从数据中心中的Oracle通过Internet复制到RDS for Oracle数据库。

验证数据迁移是否完成，然后执行到Amazon Redshift的切换。

C.在Amazon EC2实例上安装Oracle数据库软件。

为了最大程度地减少迁移时间，请通过配置1 Gbps AWS Direct Connect连接来配置AWS与公司数据中心之间的VPN连接。

将运行在Amazon EC2上的Oracle数据库配置为数据中心Oracle数据库的只读副本。在公司的本地数据中心和Amazon EC2上的Oracle数据库之间启动同步过程。

当Amazon EC2上的Oracle数据库与本地数据库同步时，创建一个AWS DMS正在进行的复制任务，以将数据从Amazon EC2上运行的Oracle数据库只读副本迁移到Amazon Redshift。

确认数据迁移已完成，然后执行到Amazon Redshift的切换。

D.创建一个AWS Snowball导入作业。使用提取代理在公司数据中心中配置服务器。

使用AWS SCT管理提取代理，并将Oracle架构转换为Amazon Redshift架构。

使用注册的数据提取代理在AWS SCT中创建一个新项目。

在AWS SCT中创建本地任务和AWS DMS任务，并复制正在进行的更改。将数据复制到Snowball设备，然后将Snowball设备返回到AWS。

允许AWS DMS将数据从Amazon S3复制到Amazon Redshift。

验证数据迁移已完成，然后执行到Amazon Redshift的切换。

QUESTION 41

A solutions architect is designing a disaster recovery strategy for a three-tier application. The application has an RTO of 30 minutes and an RPO of 5 minutes for the data tier. The application and web tiers are stateless and leverage a fleet of Amazon EC2 instances. The data tier consists of a 50 TB Amazon Aurora database.

Which combination of steps satisfies the RTO and RPO requirements while optimizing costs? (Choose two.)

Create daily snapshots of the EC2 instances and replicate the snapshots to another Region.

Deploy a hot standby of the application to another Region.

Create snapshots of the Aurora database every 5 minutes.

Create a cross-Region Aurora Replica of the database.

Create an AWS Backup job to replicate data to another Region.

Answer: BD

解决方案架构师正在为三层应用程序设计灾难恢复策略。 该应用程序的数据层的RTO为30分钟，RPO为5分钟。 应用程序和Web层是无状态的，并利用了一系列Amazon EC2实例。 数据层由一个50 TB的Amazon Aurora数据库组成。

在优化成本的同时，哪些步骤可以满足RTO和RPO的要求？ （选择两个。）

A.创建EC2实例的每日快照，然后将快照复制到另一个区域。

B.将应用程序的热备用部署到另一个区域。

C.每5分钟创建一次Aurora数据库的快照。

D.创建数据库的跨区域Aurora副本。

E.创建一个AWS Backup作业以将数据复制到另一个区域。