使用Amazon Redshift Spectrum，您可以高效地从Amazon S3中的文件中查询和检索结构化和半结构化数据，而无需将数据加载到Amazon Redshift表中。

Amazon Elastic MapReduce（Amazon EMR）是一种web服务，可以轻松快速且经济高效地处理大量数据。[需使用EC2实例可伸缩集群]

Kinesis Data Streams可用于从服务器、桌面和移动设备等来源收集日志和事件数据。

RDS Multi-AZ遵循同步复制，在一个区域内至少跨越两个可用区。读副本遵循异步复制，可以是可用分区内、跨az内或跨区域内

在发生故障转移时，Amazon RDS将提升具有最高优先级（最低编号层）的读副本。如果两个或多个Aurora Replicas共享相同的优先级，那么Amazon RDS将提升大小最大的副本。

Amazon ElastiCache for Redis不能用作DynamoDB的缓存层。[支持复制、高可用性和集群分片]
Amazon ElastiCache for Memcached是Amazon RDS或Amazon DynamoDB等数据存储的理想前端，为具有极高请求率和/或低延迟需求的应用程序提供高性能中间层。[创建会话存储很容易]

在重新平衡时，Amazon EC2 Auto Scaling会在终止旧实例之前启动新实例，因此重新平衡不会影响应用程序的性能或可用性。Amazon EC2 Auto Scaling创建了一个新的伸缩活动，用于终止不健康的实例，然后终止它。稍后，另一个伸缩活动启动一个新实例来替换终止的实例。

ELB不能将进入的流量分配给部署在不同区域的目标。[同一区域不同可用区可以]

RDS升级到数据库引擎级别需要停机时间。

S3 intelligent - tierering存储类旨在通过自动将数据移动到最具成本效益的访问层来优化成本，而不会对性能产生影响或产生操作开销。工作原理是将对象存储在两个访问层中：一个层为频繁访问而优化，另一个低成本层为不频繁访问而优化。

ElastiCache for Redis支持复制、高可用性和集群分片。

要使用CloudFront安全地提供这些私有内容，可以执行以下操作：要求您的用户通过使用特殊的CloudFront签名url或签名cookie访问您的私有内容。

EC2集群放置组将实例打包在一个可用区域内[低网络延迟、高网络吞吐量], 扩展放置组是一组实例每个实例放置在不同的机架上[减少相关的故障,Hadoop、Cassandra和Kafka],分区放置组跨逻辑分区分布实例[通常用于大型分布式和复制工作负载]

弹性结构适配器（EFA）是Amazon EC2实例的网络接口，它使客户能够在AWS上运行需要高级别节点间通信的应用程序。

Amazon FSx支持使用微软的分布式文件系统（DFS）将共享组织到一个最大可达数百PB大小的文件夹结构中。

Amazon FSx for Lustre使启动和运行世界上最流行的高性能文件系统变得简单和经济有效。用于机

器学习、高性能计算（HPC）、视频处理和金融建模等工作负载。

Global Tables在您选择的AWS区域中自动复制您的Amazon DynamoDB表。

通过启动模板，使用按需实例和现场实例跨多个实例类型提供容量

弹性负载均衡不能跨区域工作。

Amazon RDS Multi-AZ部署为RDS数据库（DB）实例提供了增强的可用性和持久性
Amazon RDS Read Replicas为RDS数据库实例提供了增强的性能和持久性。

缺省安全组的缺省规则如下：允许属于同一安全组的网络接口（及其关联实例）的流量入局。允许所有出站流量

AWS WAF允许您创建阻止常见攻击模式（如SQL注入或跨站点脚本）的安全规则，以及过滤掉您定义的特定流量模式的规则，从而控制流量到达您的应用程序的方式。

AWS安全中心(AWS Security Hub)可让您全面了解AWS帐户中的高优先级安全警报和安全状态。
AWS防火墙管理器(AWS Firewall Manager)是一项安全管理服务，允许您在AWS组织中集中配置和管理跨帐户和应用程序的防火墙规则。

VPC端点可以将VPC私有地连接到支持的AWS服务和由AWS PrivateLink提供支持的VPC端点服务
传输网关是一种网络传输集线器，您可以使用它来连接VPC和本地网络

Amazon S3支持以下发布事件的目的地：Amazon Simple Notification Service （Amazon SNS）主题Amazon Simple Queue Service （Amazon SQS）队列AWS Lambda
标准SQS队列仅被允许作为Amazon S3事件通知目的地，而FIFO SQS队列不被允许。

Amazon S3为覆盖所有区域的put和delete提供了最终的一致性。[可能读旧数据]

S3网站地址:bucket.s3-website(./-)Region

Amazon Elastic Block Store （EBS）是一种易于使用的高性能块存储服务，专为Amazon Elastic Compute Cloud （EC2）设计，可用于任何规模的吞吐量和事务密集型工作负载。默认情况下，在实例终止时删除由Amazon EBS支持的AMI的根卷。

S3 Glacier Deep Archive比S3 Glacier便宜75%，并在12小时内提供检索

SQS队列不会删除任何消息，除非超过默认的4天保留期。

Amazon Kinesis Data Streams （KDS）是一个大规模可扩展且持久的实时数据流服务。[需要手动管理分片]
Amazon Kinesis Data Firehose是可靠地将流数据加载到数据湖、数据存储和分析工具中最简单的方法。可以捕获、转换流数据[完全托管的服务，可以自动扩展以匹配数据的吞吐量]

FIFO队列支持最多每秒3000条消息（带批处理），或最多每秒300条消息（每秒300次发送、接收或删除操作）,FIFO队列的名称必须以.FIFO后缀结尾

AWS Snowball Edge适用于离线数据传输，适用于带宽受限或从远程、断开连接或恶劣环境传输数据的客户。不能支持自动和加速在线数据传输。

AWS Transfer Family为直接进出Amazon S3的文件传输提供了完全托管的支持。不支持迁移到给定用例中提到的其他AWS存储服务

AWS存储网关的文件接口或文件网关为您提供了一种无缝连接到云的方式，将应用程序数据文件和备份映像作为持久对象存储在Amazon S3云存储上。可以用于本地应用程序，以及需要通过文件协议访问S3对象存储的基于Amazon ec2的应用程序。

AWS数据库迁移服务可帮助您快速安全地将数据库迁移到AWS（将数据流式传输到Amazon Redshift和Amazon S3）,源数据库在迁移期间保持完全可操作,减少停机时间

数据库异构：使用AWS模式转换工具转换源模式和代码以匹配目标数据库的模式和代码，然后使用AWS数据库迁移服务将数据从源数据库迁移到目标数据库。

Amazon Kinesis Data Firehose是将流数据加载到数据存储和分析工具中最简单的方法。

Kinesis Data Analytics是实时分析流数据最简单的方法。

Amazon SQS的VPC端点由AWS PrivateLink提供支持

NAT实例用于向私有子网中的任何实例提供internet访问

CloudFront提高了可缓存内容（如图像和视频）和动态内容（如API加速和动态站点交付）的性能。Global Accelerator通过将边缘的数据包代理到在一个或多个AWS区域中运行的应用程序，从而提高了通过TCP或UDP的各种应用程序的性能。Global Accelerator非常适合非HTTP用例，例如游戏（UDP）、物联网（MQTT）或IP语音，以及特别需要静态IP地址或确定性快速区域故障转移的HTTP用例。这两种服务都与AWS Shield集成，实现DDoS防护。

Internet网关有两个目的：在VPC路由表中为可访问Internet的流量提供目标，并为已分配公网IPv4地址的实例执行网络地址转换（NAT）。

NAT实例可以用作堡垒服务器，安全组可以与NAT实例关联，NAT实例支持端口转发

默认情况下，在创建启动模板或使用AWS Management Console创建启动配置时启用基本监控。在使用AWS CLI或SDK创建启动配置时，默认情况下启用详细监控。

Route 53对AWS资源的别名查询不收费，但Route 53对CNAME查询收费。别名记录只能将查询重定向到选定的AWS资源，CNAME记录可以将DNS查询重定向到任何DNS记录。

对于SQS不能让相同的消息在几个小时后被多个消费者以相同的顺序使用

创建启动配置时，实例放置租赁的默认值为空，由VPC的租赁属性控制。（如果启动配置租赁或VPC租赁被设置为专用，则实例租赁也是专用的）

如果您有多个AWS站点到站点VPN连接，可以使用AWS VPN CloudHub在站点之间提供安全通信。

Elastic Fabric Adapter (EFA) 是一种网络设备，将其附加到Amazon EC2实例上，以加速高性能计算（HPC）和机器学习应用程序。

ENI （Elastic Network Interface）是VPC中的一个逻辑网络组件，代表虚拟网卡。创建网络接口，将其附加到实例，将其与实例分离，并将其附加到另一个实例。

Amazon Simple Queue Service（SQS）延迟队列允许您将新消息传递到队列延迟几秒钟。可见性超时是Amazon SQS阻止其他消费者接收和处理给定消息的一段时间。

Amazon Cloud Directory是一个云原生目录，可以存储数亿个具有多种关系和模式的特定于应用程序的对象。需要为应用程序的分层数据提供高度可伸缩的目录存储

如果您只需要允许本地用户使用其Active Directory凭据登录AWS应用程序，则应该使用AD连接器。AWS Managed Microsoft AD还允许您在AWS云中运行目录感知工作负载。如果您有超过5,000个用户，并且需要在AWS托管目录和本地目录之间建立信任关系，则AWS Managed Microsoft AD是您的最佳选择。简单AD是最便宜的选择，如果你有5000或更少的用户，并且不需要更高级的Microsoft Active Directory功能

CloudTrail可以记录、持续监控和保留与AWS基础设施中的操作相关的帐户活动。

CloudWatch：考虑资源性能监控、事件和警报
CloudTrail：考虑特定于账户的活动和审计
Config：考虑特定资源的历史记录、审计和遵从性

使用存储卷，您的整个数据卷都可以在本地网关中使用，以实现快速读取访问。使用缓存卷，AWS卷网关将完整的卷存储在其Amazon S3服务桶中，并且仅将最近访问的数据保留在网关的本地缓存中

Elasticache用作缓存层，不是一个完全托管的NoSQL数据库。

Amazon DynamoDB是一个键值和文档数据库，在任何规模下都能提供一位数的毫秒级性能。是一个完全托管、多区域、多主、持久的数据库，具有内置的安全性、备份和恢复功能，以及用于互联网规模应用程序的内存缓存。DAX是一种与dynamodb兼容的缓存服务，能够从要求苛刻的应用程序的快速内存性能中获益。

Amazon SQS提供短轮询和长轮询来从队列接收消息。默认情况下，队列使用短轮询。使用短轮询，Amazon SQS会立即发送响应，即使查询没有发现任何消息。对于长轮询，Amazon SQS在收集到至少一条可用消息后发送响应，最多不超过请求中指定的最大消息数，可以降低使用SQS的成本，因为可以减少空接收的数量。

如果需要从本地网络中解析对AWS VPC中资源的DNS查询，可以在Route 53 Resolver上创建入站端点，然后本地网络中的DNS解析器可以通过该端点将DNS查询转发给Route 53 Resolver。要从AWS VPC中解析对本地网络中任何资源的DNS查询，您可以在Route 53 Resolver上创建一个出站端点，然后Route 53 Resolver可以有条件地通过该端点将查询转发给本地网络中的解析器。

AWS CloudFormation StackSet扩展了堆栈的功能，使您能够通过一次操作跨多个帐户和区域创

建、更新或删除堆栈。堆栈集允许您通过使用单个AWS CloudFormation模板在跨区域的AWS帐户中创建堆栈。CloudFormation模板不能用于跨AWS账户和区域部署相同的模板。

由于多个应用程序并发地使用相同的流，SQS Standard和SQS FIFO都不适合给定的用例。

S3 Glacier vault是一个用于存储档案的容器。创建保险库时，需要指定保险库名称和要在其中创建保险库的AWS区域。S3 Glacier Vault Lock允许您使用保险库锁定策略轻松部署和执行单个S3 Glacier保险库的合规性控制。

使用Amazon Kinesis Data Firehose将流数据加载到数据湖、数据存储和分析工具中。可以捕获、转换和加载流数据到Amazon S3、Amazon Redshift、Amazon Elasticsearch Service和Splunk。

实例存储为实例提供临时块级存储。[不能持久化]

ALB不能基于地理匹配条件或基于IP的条件阻止或允许流量。[基于HTTP和HTTPS]

元数据（可以包含在对象中）在存储在Amazon S3上时不加密。

AWS Trusted Advisor是一种在线工具，它借鉴了从AWS为数十万AWS客户提供服务的汇总运营历史中获得的[提供最佳实践]。

AWS DataSync是一项在线数据传输服务，可通过互联网或AWS Direct Connect简化、自动化和加速从AWS存储服务中复制大量数据。

Lightsail是一个易于使用的云平台，为您提供构建应用程序或网站所需的一切，以及具有成本效益的月度计划。Lightsail提供了几种预配置的、一键启动的操作系统、开发堆栈和web应用程序

AWS Elastic Beanstalk是一个易于使用的服务，用于在熟悉的服务器上部署和扩展使用Java。

Spot实例请求可以是一次性的，也可以是持久的。如果现场请求是持久的，则在您的现场实例中断后再次打开该请求。如果请求是持久的，并且您停止了您的Spot实例，则该请求仅在您启动Spot实例后打开。
Spot blocks被设计为不被中断。

要确保弹性负载均衡器停止向正在注销或不健康的实例发送请求，同时保持现有连接打开，请使用connection draining

可以跨AWS区域复制AMI，可以与另一个AWS帐户共享AMI，复制由加密快照支持的AMI不会导致未加密的目标快照

文件网关允许您在Amazon S3中使用文件协议（如网络文件系统（NFS）和服务器消息块（SMB））存储和检索对象。EFS、EBS和S3不支持SMB

恢复后的实例与原实例完全相同，包括实例ID、私有IP地址、弹性IP地址和所有实例元数据，恢复后将保留该公共IPv4地址

Amazon RDS不提供自动扩展功能，因此不适合给定的用例。

如果一个用户或角色有一个IAM权限策略，授予了一个操作的访问权限，而该操作是不被适用的scp允许或明确拒绝的，则该用户或角色不能执行该操作，scp影响附加帐户中的所有用户和角色，包括根用户，scp不影响服务链接的角色

EC2 hibernate允许重新加载休眠实例的RAM内容并恢复先前运行的进程

Amazon S3 Glacier使用高级加密标准（AES） 256位对称密钥自动加密静态数据，并支持通过安全套接字层（SSL）安全传输数据。

AWS建议使用Snowmobile在单个位置迁移10PB或更多的大型数据集。对于小于10PB或分布在多个位置的数据集，应该使用Snowball。

EFS提供POSIX兼容的文件存储解决，S3不提供

IAM权限边界。只能应用于角色或用户，不能应用于IAM组。

在Kinesis Data Stream中，只能拥有与分片相同数量的消费者

Linux实例上挂载一个网络文件系统需要排除Glacier Deep Archive和S3 Intelligent Tiering

启动模板确实支持按需（On-Demand）和Spot实例的混合，ASG获得了自动伸缩功能。

KMS是加密服务，不是秘密存储

s3:ListBucket应用于桶，s3:GetObject应用于桶内的对象

OLTP =>关系数据库

为AZ间的数据传输付费，而在单个AZ内传输数据是免费的。

S3 select不能用于获取文件的第一个字节。

弹性IP一次只能附加到一个EC2实例

Bastion Hosts正在使用SSH协议，这是端口22上基于TCP的协议。应该使用Network Load Balancer

具有desired=2的ASG将创建两个实例

CloudWatch Events不能调用EC2实例上的应用程序

使用私有IP，这样网络保持私有，成本最低

AWS DMS主要设计用于数据库迁移

AWS Backup是一项服务，简化并集中管理AWS资源的备份

S3网关端点是一个VPC端点，允许EC2实例在不经过互联网的情况下访问S3服务。

DynamoDB点对点恢复，允许进行连续备份，并能够在最后35天内的任何时间点恢复表。

NAT网关用于允许私有子网中的实例连接到internet，同时阻止来自internet的入站流量到达它们。

AWS Glue作业书签是一个功能，允许ETL作业跟踪在先前运行中已经处理过的数据。

AWS Snowball Edge存储优化设备允许在最小的网络带宽需求下大量数据进出AWS的传输。

AWS Firewall Manager允许跨多个账户和地区的安全规则集中管理，简化了保护资源的过程。

EC2现货实例允许用户竞标亚马逊的多余EC2计算能力，可以是解决无状态、可随时启动和停止的作业的具有成本效益的解决方案。

文件不会通过S3 URL直接访问： 通过创建原始访问身份（OAI）并将其分配给CloudFront分发，同时配置S3存储桶，以便只有OAI具有读取权限

S3 Object Lock合规模式和治理模式区别?

Amazon FSx for Lustre是为HPC工作负载设计的高性能文件系统，可以与Amazon S3集成进行长期存储。

在根组织单位中创建服务控制策略（SCP）允许安全团队设置适用于组织内所有账户的权限。

AWS Shield Advanced为在AWS上运行的应用程序提供DDoS保护，包括通过应用程序负载均衡器提供的应用程序。

通过在应用程序负载均衡器上配置AWS WAF（Web应用程序防火墙），架构师可以创建基于地理位置的访问控制规则，根据访问者的国家允许或阻止流量。

配置CloudFront字段级加密配置文件提供了额外的安全层，确保敏感数据被加密，并且只能由具有必要凭据的特定应用程序解密。

Amazon DynamoDB加速器（DAX）是一个内存缓存，可以显著提高DynamoDB表的读取性能，而无需对应用程序进行更改。

AWS Transfer Family是一个完全托管的服务，可用于设置和运行SFTP服务器

AWS Elastic Beanstalk是一个完全托管的服务，可以自动处理Web应用程序的部署、扩展和监控。

Amazon Transcribe可以用于多个扬声器识别

Amazon Pinpoint可用于发送SMS消息

AWS Lake Formation提供了一个集中的存储库，用于管理数据分析资源

AWS资源组标签编辑器允许根据其标签在所有AWS服务和区域中搜索和报告资源

AWS WAF（Web应用程序防火墙）可以配置为过滤恶意流量

Amazon Redshift集群中，这是一个完全托管的PB级数据仓库服务，支持使用SQL进行按需分析。

EFS是一个可扩展的文件存储服务，用于与AWS云服务一起使用，可以被多个EC2实例同时访问。

Kinesis Data Firehose可以自动加密数据，当数据被摄取时，以指定的Parquet格式将其存储在S3中。

Amazon Aurora全局数据库进行热备用部署设置允许全局数据库不断更新，并在发生灾难时快速提升以处理流量。

使用AWS CloudFormation自动化次要AWS区域的基础设施部署，设置可以快速使用CloudFormation模板激活

Amazon QuickSight可视化结果，这是一个商业分析服务，可以创建可视化效果、报告和仪表板

Amazon FSx for NetApp ONTAP是一个完全托管的服务，提供了一个高度可用的文件系统，支持NFS和SMB协议，适用于Linux和Windows环境。

从计费仪表板下载账单，不提供按用户列出计费项目的粒度。

Amazon EBS是块存储，不提供文件系统共享功能。EBS卷一次只能附加到单个EC2实例

存储卷网关保留了本地的全部数据集，并异步地将数据备份到AWS，确保在数据安全传输和存储在云中的同时保持了本地访问。

AWS Snowball，是为数据迁移而非持续的备份解决方案设计的，并且不维护本地访问。

AWS Snowball Edge，提供数据传输和边缘计算能力，但主要用于一次性或不频繁的数据传输。

缓存卷网关，只缓存频繁访问的数据，不适合维护对所有数据的本地访问。

S3 Object Lambda允许自定义代码在每次从S3获取对象时执行

AWS不支持跨多个可用区的子网

Amazon FSx for Lustre文件系统是专为计算密集型工作负载设计的高性能文件系统，适用于研究实验室和高性能计算

AWS存储网关文件网关，用于低延迟访问存储在S3中的文件

AWS Snowcone，旨在将大量数据导入AWS，但每个设备限8TB

Fargate不需要管理EC2实例

AWS DMS主要用于数据库迁移和复制，而不是用于一般文件系统数据传输

EC2 集群放置组旨在为需要高水平网络连接和低延迟的应用程序优化性能。

Amazon S3缓存卷配置旨在提供对最常用数据的低延迟访问，而较少访问的数据存储在云端。存储卷，将在本地存储整个数据集。

S3存储镜头提供详细的指标和对S3存储桶使用模式的洞察

Amazon Inspector是一项安全评估服务，可以自动识别在EC2实例上运行的应用程序中的漏洞和安全问题。

AWS Glue是一个完全托管的ETL服务

会话管理器是一个完全托管的服务，提供安全和可审计的实例管理

Kinesis数据分析可用于低延迟查询数据。Kinesis数据流具有默认的持久数据存储

为了确保所有上传到Amazon S3存储桶的对象都已加密，解决方案架构师应更新存储桶策略，以拒绝任何没有设置　x-amz-server-side-encryption头的PutObject请求，强制使用服务器端加密

Amazon DynamoDB表中，这是一个可扩展且高度可用的NoSQL数据库服务

AWS Snowball是一项Petabyte规模的数据迁移服务

Amazon EBS快照快速恢复功能，并使用快照预置AMI，允许从快照快速恢复EBS卷，从而减少了从AMI初始化实例所需的时间

Secrets Manager提供了一种安全的方式来存储、管理和检索数据库凭据。

为了解决SQL注入漏洞，公司应该在应用程序负载均衡器（ALB）前使用AWS WAF（Web应用程序防火墙）。

AWS Lake Formation可用于对QuickSight用户执行列级访问控制。

Amazon S3文件网关。这种类型的存储网关提供文件系统接口访问S3中存储的对象，支持SMB和NFS协议

计算节省计划提供了显著的计算使用节省，并允许在相同的实例族内更改实例类型

gp2卷可以自动扩展到每个1TB存储的3000 IOPS

RDS　Proxy可以更有效地管理数据库连接

接口端点是VPC端点，允许流量在VPC和AWS服务之间流动，无需使用公共互联网路由。

Amazon DynamoDB非关系型数据库

满足高可用性、POSIX　兼容、最大数据持久性和跨EC2实例共享要求的最具成本效益的解决方案是使用Amazon弹性文件系统（EFS）标准存储类别

对最小权限访问的策略，创建安全组

io2卷类型旨在满足高IOPS需求，并提供一致和可预测的性能，非常适合数据库工作负载。

gp3提供具有基线和最大IOPS的突发性能

CloudTrail是一项服务，提供用户、角色或AWS服务所采取行动的记录