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[复制和存档快照]、高可用性和集群分片，不支持多线程]
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，支持多线程，关系型数据库]
DAX不能用作关系数据库的缓存层。

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，单实例应该用弹性IP，ALB贵

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[无服务器环境]

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

EBS数据在实例终止或重新启动后仍然存在。EFS是一个网络驱动器，最后，S3不能作为本地磁盘（本机）挂载。

SES是一个电子邮件发送服务。SNS是一种通知服务

由于AMI在创建的区域内受到限制，因此需要跨区域复制，以便进行灾难恢复

ElastiCache不支持IAM Auth。只有Redis Auth有助于用户名/密码的安全性

Neptune图形数据库

ASG会平衡AZ，然后终止该AZ内具有最旧启动配置的实例。

Amazon SageMaker 是一个完全托管的服务，使开发人员和数据科学家能够快速高效地构建、训练和部署ML模型。另一方面，Amazon QuickSight是一个商业分析服务，可以用来创建可视化、报告和仪表板。可以轻松地与SageMaker集成，以可视化由ML模型处理的数据。

Amazon WorkSpaces是一个托管的、安全的云桌面服务。

启动配置是不可变的，意味着不能更新。

使用VPC端点网关的两个服务是Amazon S3和DynamoDB。其余为“VPC端点接口”：SQS、SNS和Kinesis

灾难恢复不丢失任何重要记录，发生灾难时按需创建非关键系统：Pilot Light

Multi-AZ意味着URL是相同的，故障转移是自动的，CNAME将自动更新到指向备用数据库的点。

基于路径的路由和基于主机的路由仅适用于应用程序负载均衡器（ALB）

EFS不会改变任何东西，因为EFS上的静态内容仍然需要由ECS实例分发

EFS没有得到S3的显式支持

仅限出口的Internet网关支持IPv6，不支持IPv4。Internet网关必须部署在公网子网中，用于VPC和互联网之间的通信。

使用SSE-C，公司仍然可以提供加密密钥，但让AWS进行加密

创建IGW后，请确保更新路由表。请确保安全组允许ping请求使用ICMP协议

在VPC中部署Lambda或加强安全组不会改变身份验证层

Glue用于执行ETL，但不能运行自定义Python脚本。Kinesis Streams是用于实时数据的

CloudFormation允许您将基础架构保留为代码，并重用公司周围的最佳实践来进行配置参数。

CloudFront在这里不是一个好的解决方案，因为内容是高度动态的，而且CloudFront会缓存内容。动态应用程序不能部署到S3

DynamoDB Streams将包含发生在DynamoDB表上的所有更改的流。

Redshift优化成本：
将数据移动到S3 glacier，Redshift将无法查询它。
应该将数据迁移到S3 IA，并使用Athena（S3之上的无服务器SQL查询引擎）来分析冷数据。

Athena是无服务器SQL，Redshift是SQL

生成S3预签名URL将绕过CloudFront，因此应该使用CloudFront签名URL。DynamoDB触发器或API Gateway作为服务不能用于生成这些预签名的url。

CloudFront分发不支持附加IAM角色。S3存储桶没有安全组。

在不增加gp2卷大小的情况下，不能直接增加gp2卷上的IOPS

3个AZ要有2个实例保持可用性

弹性IP地址是分配给您的AWS帐户的静态、公共IPv4地址。使用弹性IP地址，可以通过快速将地址重新映射到帐户中的另一个实例来掩盖实例或软件的故障。

API网关设置了对稳态速率和针对您帐户中所有API的请求提交的爆发的限制。

Amazon Gateway Endpoint在路由表中指定路由目标的网关，用于发送到受支持的AWS服务的流量。

AWS WAF预配置的保护来阻止常见的攻击，如SQL注入或跨站点脚本。

Amazon Aurora Global Database是为全球分布式应用程序设计的，允许单个Amazon Aurora数据库跨越多个AWS区域。

在将对象从S3 Standard/S3 Standard-IA过渡到S3 Standard-IA/S3 One Zone-IA之前，最小存储持续时间为30天。

Amazon GuardDuty提供威胁检测功能，能够持续监控和保护存储在Amazon S3中的AWS帐户、工作负载和数据。GuardDuty分析帐户和网络活动中生成的连续元数据流，这些数据流位于AWS

CloudTrail事件、Amazon VPC流日志和DNS日志中。还使用集成的威胁情报，如已知的恶意IP地址，异常检测和机器学习，以更准确地识别威胁。在常规设置中禁用服务—在放弃服务权限和重置服务之前，禁用服务将删除所有剩余数据，包括您的发现和配置。使用机器学习、异常检测和集成威胁情报来识别潜在威胁并确定优先级。

一个组不能有来自另一个AWS帐户的用户，不能将策略应用于其他帐户的IAM用户来解决；对于跨帐户访问，需要添加一个策略，该策略的主体（而不是资源）是希望授予权限的AWS帐户。

AWS Lambda可以跨帐户写入，并且SNS主题不能订阅另一个SNS主题。SES不能直接写入Kinesis数据流。

Amazon S3中的桶策略可用于在单个桶内的部分或全部对象之间添加或拒绝权限。可以将策略附加到用户、组或Amazon S3桶上，实现对权限的集中管理。通过桶策略，您可以授权AWS帐户或其他AWS帐户中的用户访问您的Amazon S3资源。

使用IAM策略，您只能向您自己的AWS帐户中的用户授予访问您的Amazon S3资源的权限。使用acl，您只能授权其他AWS帐户（而不是特定用户）访问您的Amazon S3资源。桶所有者帐户可以将权限委托给自己帐户中的用户，但不能将权限委托给其他AWS帐户，因为不支持跨帐户委托。

通过Cognito用户池为您的应用程序负载均衡器使用Cognito身份验证，特定于应用程序的用户身份验证可以通过Cognito用户池提供。Amazon Cognito身份池为来宾（未经身份验证）用户和已经过身份验证并收到令牌的用户提供临时AWS凭据。

Amazon EC2 Auto Scaling不会立即终止处于受损状态的实例。Amazon EC2 Auto Scaling还可能延迟或不终止那些无法为状态检查报告数据的实例。当组的健康检查配置设置为EC2时，Amazon EC2 Auto Scaling不使用ELB健康检查的结果来确定实例的健康状态。

User Data通常用于执行常见的自动化配置任务，甚至在实例启动后运行脚本。在Amazon EC2中启动实例时，可以传递两种类型的用户数据——shell脚本和cloud-init指令。默认情况下，以user数据输入的脚本以root用户权限执行，用户数据仅在首次启动实例时的启动周期中运行

私有托管区域需要配置DNS主机名和DNS解析—私有托管区域需要配置DNS主机名和DNS解析。如果您有一个私有托管区域和一个为相同域名路由流量到您的网络的Resolver规则，则Resolver规则优先。

使用集中式VPC端点连接多个VPC，也称为共享业务VPC—VPC端点可以将VPC私有连接到支持的AWS服务，无需Internet网关、NAT设备、VPN连接或AWS直连连接。
Transit VPC在专用的公网网关的Transit VPC中使用客户管理的Amazon EC2 (Amazon Elastic Compute Cloud) VPN实例
AWS建议每个VPC最多125个对等连接。

AWS Global Accelerator使用端点权重来确定定向到端点组中端点的流量比例，并使用流量拨号来控制定向到端点组（部署应用程序的AWS区域）的流量百分比。[蓝绿发布]

专用主机：软件证书

专用实例：客户机的单租户硬件需求

默认情况下，Lambda函数总是在AWS拥有的VPC中运行，因此可以访问任何公共互联网地址或公共AWS api。Lambda功能启用VPC后，需要通过公网子网的NAT网关路由访问公共资源。Lambda功能始终在aws所属的VPC中运行。当需要与私有子网内的私有资源进行交互时，才需要开启VPC访问功能。如果您打算在多个Lambda函数中重用代码，您应该考虑为可重用代码创建一个Lambda层——您可以配置Lambda函数以层的形式拉入额外的代码和内容。一个函数一次最多可以使用5个层。支持基于资源的策略，用于向特定AWS帐户、AWS组织或所有帐户授予层使用权限。解压缩后的功能和所有层的总大小不能超过解压缩后的部署包大小限制250mb。Lambda根据分配给函数的内存比例分配计算能力。这意味着您可以过度配置内存以更快地运行功能，并可能降低成本。AWS建议您不要过度配置功能超时设置。

AWS DMS使您能够将数据从受支持的源无缝迁移到AWS云中的关系数据库、数据仓库、流媒体平台和其他数据存储。（Amazon S3流到Amazon Kinesis data Streams）
S3不能直接将数据写入SNS，尽管它可以使用S3事件通知将事件发送到SNS。SNS也不能直接向Kinesis Data Streams发送消息。
AWS Transit Gateway允许客户将其Amazon vpc和本地网络连接到单个网关。
使用“Transit VPC”实现不同地区的VPC与客户数据中心之间的互通。可以使用此功能将地理位置不同和/或运行在单独AWS帐户中的多个VPC连接到一个通用VPC，该VPC充当全球网络传输中心。
VPC内的资源无法通过对端VPC的混合连通性到达本地。

对于存储在Amazon S3中的静态应用程序数据，可以利用跨区域复制（Cross-Region Replication，CRR），允许数据在其他区域也可用。
使用EFS File Sync将文件及其相应的元数据快速复制到另一个区域。
对于操作系统映像，在使用Amazon EC2和Amazon EBS时，必须手动启动复制，并确保在备用区域中复制了适当的Amazon Machine images （ami）并可用。
Amazon EBS卷的范围局限于单个可用分区[单可用区]。对于附加到您的计算资源的Amazon EBS卷，在另一个区域创建快照将允许本地卷的数据在另一个区域可用。

AWS成本资源管理器（AWS Cost Explorer Resource Optimization）可帮助您识别未充分利用的EC2实例
AWS Compute Optimizer为您的工作负载推荐最优的AWS Compute资源，通过使用机器学习分析历史利用率指标来降低成本并提高性能。帮助您根据利用率数据选择最优的Amazon EC2实例类型，不推荐实例购买选项
S3存储类分析（Amazon S3 Analytics Storage Class analysis）没有给出过渡到ONEZONE_IA或S3 Glacier存储类的建议。
可信顾问（AWS Trusted Advisor）没有自动更新保留实例的功能。

AWS X-Ray可以帮助开发人员分析和调试产品、分布式应用程序，跨AWS帐户收集数据。

VPC流量日志：记录VPC中各网络接口的IP流量信息。流量日志数据用于分析网络轨迹，有助于网络安全。

当数据保留、最小停机时间和应用程序性能是优先级时，Multi-AZ是最佳选择。读取副本用于缓解来

自主数据库的读取流量，它本身不能用作完整的容错解决方案。

当你想要构建一个应用程序来响应来自[SaaS应用程序和/或AWS服务的事件]时，推荐使用Amazon EventBridge。Amazon EventBridge是唯一一个直接与[第三方SaaS合作伙伴]集成的基于事件的服务。Amazon EventBridge还自动从90多个AWS服务中获取事件，而不需要开发人员在其帐户中创建任何资源。使用Eventbridge，下游应用程序需要在事件到达时立即处理事件，从而使其成为一个紧密耦合的场景。

AWS DayaSync只支持NFS和SMB文件类型，不支持磁带

如果您的对象小于1GB，或者数据集的大小小于1GB，则应该考虑使用Amazon CloudFront的PUT/POST命令以获得最佳性能。给定用例的数据大于1GB，因此S3传输加速是更好的选择。

CloudWatch恢复选项仅适用于系统检查失败，而不适用于实例状态检查失败。此外，如果终止实例，则无法恢复实例。不能使用CloudWatch事件直接触发EC2实例的恢复。恢复操作只支持配置了EBS卷的实例，实例存储卷不支持CloudWatch告警自动恢复。Trusted Advisor本身不支持EC2实例的运行状况检查或恢复。

Amazon SNS遵循“发布-订阅”（pub-sub）消息传递范式，使用“推送”机制将通知传递给客户端。这是SNS和SQS的一个重要区别。SQS是一种轮询机制，它为应用程序提供了自行轮询的机会，而推送机制则假定其他应用程序存在。

Amazon RDS仅支持向后兼容的磁存储。AWS建议您使用通用SSD或预置IOPS来满足任何存储需求。无法从备用数据库中读取数据

Amazon FSx for Lustre和Amazon Elastic File System只适用于Linux

创建NAT网关时，必须指定NAT网关所在的公网子网。

仅限出口的internet网关是指支持IPv6流量的internet网关
NAT实例不是托管服务，必须由客户管理和维护。

应用负载均衡器不能分配弹性IP地址（静态IP地址），NLB可以配置为弹性IP。不能分配一个弹性IP给一个自动伸缩组，因为ASG只管理一组EC2实例。

使用Global Accelerator，可以获得两个面向客户的全局静态ip，以简化流量管理。在后端，添加或删除AWS应用程序源，如网络负载平衡器、应用程序负载平衡器、弹性ip和EC2实例，而无需进行面向用户的更改。为了减轻端点故障，全局加速器会自动将您的流量重新路由到最近的健康可用端点。

如果您有一个正在运行实例的EC2 Auto Scaling group (ASG)，如果您选择删除该ASG，则该实例将被终止，ASG将被删除。EC2自动伸缩组可以跨越可用区，但不能跨越[AWS区域]，数据不会自动从现有实例复制到新的动态创建的实例。一次只能为EC2 Auto Scaling组指定一个启动配置，并且在创建启动配置之后不能修改启动配置。

使用Route 53 DNS故障转移，您可以在全球多个AWS区域同时运行主应用程序，并进行跨区域故障转移。

所有DynamoDB表都是在AWS拥有的客户主密钥（CMK）下加密的，它不会写入CloudTrail日志

AWS WAF可以部署在Amazon CloudFront、ALB （application Load Balancer）和Amazon API Gateway上。不能直接在EC2实例上配置。

Amazon Athena是分析工具，Quicksight不是

IAM数据库认证适用于MySQL和PostGreSQL。

Auto Scaling组可以在同一区域内的一个或多个可用分区中包含EC2实例。但是，自动伸缩组不能跨越多个区域。

一个子网一次只能关联一个路由表。子网总是与某个路由表相关联。

EBS卷是灵活的。对于当前实例类型下挂载的当前卷，可以在生产卷上动态增加卷的大小、修改发放的IOPS容量和更改卷的类型。[可用区锁定]

若要在自动缩放组中使用弹性负载平衡，请将负载平衡器附加到自动缩放组，以便向负载平衡器注册该组。

现货实例（Spot instances）是备用的EC2容量，可以为您节省90%的按需价格。Amazon EC2可以根据容量需求中断Spot实例，并发出2分钟的通知。Spot blocks允许您一次请求Amazon EC2 Spot实例1到6小时，以避免被中断。Spot Fleet是Spot实例和可选的On-Demand实例的集合或舰队。Spot Fleet尝试启动Spot实例和按需实例的数量，以满足您在Spot Fleet请求中指定的目标容量。

Kinesis Data Streams （KDS）和Kinesis Data Analytics是用于[实时处理]数据的
Redshift允许您使用复杂的查询优化、高性能本地磁盘上的列式存储和大规模并行查询执行，对pb级的结构化数据运行复杂的分析查询。大多数结果会在几秒钟内返回。[近实时]
Amazon Kinesis Data Firehose是一个自动扩展解决方案

通过AWS Firewall Manager，您可以跨组织内的帐户和资源集中配置AWS WAF规则、AWS Shield高级保护、Amazon Virtual Private Cloud （VPC）安全组、AWS Network Firewall和Amazon Route 53 Resolver DNS Firewall规则。

Amazon Inspector是一项自动安全评估服务，可以帮助您测试Amazon EC2实例的网络可访问性，以及运行在这些实例上的应用程序的安全状态。

ASG自动缩放首先终止不健康的实例，然后启动一个新实例；在重新平衡时，在终止旧实例之前启动新实例。

任何数据库引擎级别的升级都会触发主DB实例和备用DB实例同时升级。这会导致停机，直到升级完成，停机时间根据DB实例的大小而变化。

服务控制策略（SCP）是一种[组织]策略，您可以使用它来管理组织中的权限。scp提供对组织中所有帐户的最大可用权限的集中控制。scp帮助您确保您的帐户符合组织的访问控制准则。
服务链接角色是直接链接到AWS服务的唯一类型的IAM角色。服务链接的角色是由服务预定义的，包

括代表您调用其他AWS服务所需的所有权限。链接的服务还定义了如何创建、修改和删除服务链接的角色。

对于所有现有对象和新对象，以及所有区域中的所有S3 GET、PUT和LIST操作，以及更改对象标记、acl或元数据的操作，现在都是强一致的。

当临时队列不再使用时，客户机自动清理临时队列，即使使用该客户机的某些进程没有被彻底关闭。

最小化成本，需要在同一个AZ中启动Read Replica，因为必须为AZ间的数据传输付费，而在单个AZ内传输数据是免费的。

使用Amazon S3 Select，您可以通过使用ScanRange参数指定要查询的字节范围来扫描对象的子集。此功能允许您通过将工作拆分为一系列不重叠扫描范围的单独Amazon S3 Select请求来并行扫描整个对象。

AWS不建议客户使用AWS Managed VPN作为速度超过1gbps的AWS Direct Connect连接的备份。

—x-amz-acl头用于指定S3 PutObject请求中的ACL。访问权限是用这个头定义的。
Amazon S3允许HTTP和HTTPS请求。aws:SecureTransport密钥用于检查请求是通过HTTP还是HTTPS发送。当此键为true时，意味着通过HTTPS发送请求。

只支持“预置IOPS”SSD卷（Provisioned IOPS SSD volumes）的“多挂载”（Multi-Attach）功能。其他EBS卷不支持Multi-Attach

大数据分析：Amazon EMR和AWS Glue

卷网关（Volume Gateway）用于块存储，而不是用于文件存储

AWS建议您使用AWS DataSync将[现有]数据迁移到Amazon S3，不是持续复制

Amazon EFS预置吞吐量模式（Provisioned Throughput）适用于具有高吞吐量与存储（mb /s / TiB）比率的应用程序，或者需求大于突发吞吐量模式所允许的应用程序。
每个任务输出是20 MB，但是DynamoDB表中每个项目的存储限制是400 KB。

AWS建议使用单独的队列来提供工作的优先级。

实例概要文件是角色的容器，可以在启动时附加到Amazon EC2实例。一个实例概要文件只能包含一个角色，并且这个限制不能增加。

SSE-C：自己管理S3加密密钥，SSE-S3：托管密钥的服务器端加密

只能在启动实例时为实例指定实例存储卷。不能将实例存储卷从一个实例中分离出来，并将其附加到另一个实例。实例存储中的数据仅在其关联实例的生命周期内持续存在。如果实例重新启动（有意或无意），则实例存储中的数据将持续存在。当您停止、休眠或终止一个实例时，实例存储中的每个存储块都会被重置。位于物理上连接到主机的磁盘上。

NLB必须可以通过互联网访问，因此必须位于公共子网中，并将作为所有传入流量的单一联系点。

望将现有的本地目录与兼容的AWS服务一起使用时，AD连接器（AD Connector）是您的最佳选择。Simple AD不支持多因素身份验证（MFA）

只支持linux环境的Nitro EC2实例支持多挂载EBS卷。

RDS应用OS更新的方式是：在备用服务器上执行维护，然后将备用服务器提升为主服务器，最后在旧的主服务器上执行维护，旧的主服务器成为新的备用服务器[如果是数据库引擎是全部服务器关闭]，在首选备份窗口期间主服务器上的I/O活动不再挂起，因为备份是从备用服务器获取的。对DB实例的更新将跨可用区同步复制到备用服务器，以保持两者同步

SSE-KMS为您提供审计跟踪，显示您的CMK是何时被谁使用的。

要限制对您从Amazon S3 bucket提供的内容的访问：创建OAI （origin access identity）并更新S3 Bucket Policy。S3存储桶没有安全组

在不增加gp2卷大小的情况下，不能直接增加gp2卷上的IOPS

Amazon S3 Inventory可以帮助管理存储，可以按照已定义的时间表在S3 bucket中创建对象列表。

Private Link用于在帐户中由NLB前端的应用程序与另一个帐户中的弹性网络接口（ENI）之间创建私有连接，而无需VPC对等，并允许两者之间的连接保留在AWS网络中。

Shield中设置基于速率的规则，WAF可以

VPC端点使您可以将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。VPC的端点分为接口端点和网关端点两种。接口端点是一个弹性网络接口，具有来自子网的IP地址范围的私有IP地址，该IP地址用作指向受支持服务的流量的入口点。网关端点是您在路由表中为发送到受支持的AWS服务的流量指定路由目标的网关。支持以下AWS服务：Amazon S3和DynamoDB。S3和DynamoDB都不支持接口端点

使用 Amazon RDS Custom for Oracle，该服务支持数据库引擎的自定义，以适应需要特权访问的第三方特性

AWS 上的工作负载发现旨在自动发现和绘制跨多个账户和区域的资源之间的关系。

AWS Transfer Family支持AS2协议，这是安全数据传输所需的。

Amazon AppFlow是一个完全托管的服务，可以安全地在 Salesforce 和 Amazon S3 之间传输数据。支持传输中的加密，并允许使用 AWS KMS CMKs 对静态数据进行加密

AWS Lambda 允许响应S3事件运行代码

通过在私有子网中托管应用程序到 Amazon ECS 并设置私有 VPC 链接，API Gateway 可以安全地访问后端服务

出口仅限互联网网关允许 IPv6 流量从 VPC 路由到互联网，仅用于出站（出口）流量。

Amazon EFS提供了一个可扩展且[高度耐用]的文件系统，其数据可以使用 AWS Backup 备份和复制到另一个区域

DataSync 旨在自动化本地存储和 AWS 服务（如 S3）之间的数据传输，并支持在传输过程中加密数据。

S3 Glacier 是长期存档数据的低成本存储选项。加急检索可以使存档数据在最快 1-5 分钟内可用，满足公司在需要时快速访问的要求。

DynamoDB 提供了一个名为点播恢复和持续备份的功能，可以通过最少的配置启用。

Amazon Macie 是一项使用机器学习自动发现、分类和保护 AWS S3 存储桶中的敏感数据的服务。

网络ACL（访问控制列表）是控制子网级别流量的推荐方式，因为它们充当子网的防火墙。比修改各个实例的安全组更有效。

安全组可以引用另一个区域的安全组ID

Amazon Aurora按需允许开发者使用高性能数据库，该数据库可以根据需求进行扩展，并且只需支付所使用的计算能力

通过使用AWS Config，公司可以自动化识别未标记资源并对其应用标签的过程。

AWS Systems Manager支持通过Systems Manager控制台直接将会话日志发送到S3存储桶

Amazon RDS中的存储自动扩展允许数据库根据需要自动增加存储容量，无需手动干预或造成停机。

AWS服务目录允许组织创建和管理一个产品目录，这些产品被批准在组织内使用。

对于不可预测的工作负载来说，按需容量模式是成本效益的

AWS Lambda函数URL提供了一个直接的HTTP(S)端点来调用Lambda函数。

Amazon EMR可以使用其基于Hadoop的框架并行处理大量数据，非常适合存储在S3中的半结构化数据。此外，EMR可以直接与Amazon Redshift集成，通过查询和连接存储在S3中的数据与存储在Redshift中的数据，来丰富数据

AWS Control Tower提供了额外的账户和资源管理功能

EKS连接器允许注册和连接所有Kubernetes集群，包括本地集群，到Amazon EKS控制平面。

附加单个EBS卷不会提供并发访问

Amazon CloudWatch为EventBridge提供了指标，可以用来确定规则条件是否得到满足，以及目标是否被调用。

AWS证书管理器（ACM）允许创建一个可以由第三方CA签名的证书，满足公司对特定公共第三方CA的要求。

SnapStart是一个功能，可以改善Lambda函数的启动时间高达90%，而且不需要额外的费用。预留并发需要维护一定数量的实例准备响应，从而产生额外的费用。

Memcached更像是一个内存缓存系统，没有提供与Redis相同的持久性和数据管理功能。

AWS Step Functions Map状态的分布式模式，是针对存储在Amazon S3中的半结构化数据进行大规模并行处理的解决方案，具有最高的运营效率。

Lake Formation 支持可以根据这些行和单元格中的值限制对特定行和单元格的访问的数据过滤器。

配置基于 SAML 2.0 的联合，允许公司使用其现有的活动目录身份来访问 AWS 资源，而无需创建和管理单独的 IAM 用户。

DataSync 旨在自动化本地存储和 AWS 服务（如 S3）之间的数据传输，并且它包括数据完整性检查以确保数据已正确传输。

S3 存储镜头提供对跨多个账户的 S3 资源使用的洞察，并可以生成不完整多部分上传的指标，这些指标可用于成本合规性报告。

EBS通过使用快照锁定功能，公司可以防止意外删除

创建客户管理密钥并使用它来加密EBS卷，为公司提供了对加密密钥的完全控制，包括管理密钥轮换的能力。

Wavelength Zones是在电信提供商的设施内部署的AWS基础设施，将AWS服务更接近最终用户，并提供个位数毫秒的延迟。

在VPC内部署Lambda函数确保连接是安全的

地理位置路由更适合于位置特定的内容分发，故障转移和地理接近策略更侧重于可用性和地理接近性

AWS X-Ray应配置为跟踪微服务之间的请求，提供对应用程序组件交互和性能的洞察

让位于私有子网的Amazon EC2实例能够连接到公共互联网，公司应在公共子网中创建公共NAT网关

为了防止将新请求转发到过载的EC2实例，公司应该使用最少未完成请求算法

FSx for ONTAP支持SMB和NFS协议

为了在不影响运行中的应用程序的情况下对EC2实例进行修补，可以在AWS Systems Manager中启用默认主机配置管理

预测扩展使用机器学习来预测需求并相应地调整资源数量。

DynamoDB提供两种类型的读取：最终一致性读取（默认）和强一致性读取。强一致性读取确保响应包括最新数据，反映所有在读取之前收到成功响应的写入。

GuardDuty是一个威胁检测服务，持续监控恶意活动和未经授权的行为，包括不寻常的登录尝试。

EventBridge是一个无服务器事件总线，可以在响应传入事件时触发目标Lambda函数，无需额外的组件，如SNS或SQS。

为了满足加密数据传输的安全要求，解决方案架构师应该下载AWS提供的根证书，并在连接到RDS实例的所有连接中使用它们。

CloudFront没有网络ACL

正确的选择是基于身份的策略，因为它直接与用户或组相关联，确保组中的所有用户继承策略中定义的权限。

VPC Lattice服务网络允许为每个微服务定义HTTPS侦听器，并启用服务发现。

创建一个IAM角色这种方法遵循最小权限原则，并且与创建IAM用户或修改权限边界相比，被认为更安全。

QLDB是一个完全托管的分类账数据库，提供透明、不可变、可进行密码学验证的所有数据更改日志，非常适合需要高度数据完整性和可审核性的应用，如会计记录。

AWS Application Discovery Service可以自动发现并收集有关公司本地数据中心的信息，包括有关应用程序的细节、它们之间的依赖关系以及网络配置。

AWS Control Tower提供了一个集中的治理模型，并自动建立账户，包括持续遵守FSBP。

Amazon Rekognition提供了预先训练好的模型，用于图像分析，可以检测各种不想要的内容。

AWS Outposts允许您在本地数据中心运行AWS服务

Amazon S3 File Gateway将本地NFS存储迁移到AWS，该网关允许使用NFS协议的S3作为文件存储。

AWS Glue DataBrew是一个可视化、用户友好的工具，可以无需编写代码进行数据准备。支持数据转换、数据来源和数据分析。DataBrew 配方可以与其他员工共享，使协作数据转换步骤变得容易。

Amazon S3 接口端点允许流量直接从本地网络路由到 AWS 网络内的S3 服务，无需公共 VIF 或 NAT 网关。

AWS 证书管理器（ACM）为公共域名提供免费的SSL/TLS 证书。通过请求公共证书，公司可以使用自定义域名为其 CloudFront 分发，无需额外费用。

Lambda@Edge可以用于无服务器授权

AWS Glue不适合实时处理

Amazon SES 是一种可扩展且具有成本效益的电子邮件服务，旨在发送大量电子邮件。

计算节省计划涵盖了EC2和Lambda的使用。

GP3卷提供了性能和成本的平衡，允许最多16，000 IOPS

合规保留模式确保数据在保留期限内不能被删除或覆盖

AWS Direct Connect连接主要用于建立本地与AWS的专用连接