SAA 考点 @2019-08-13

注: 一些过于 basic 的没有记录, 例如基本的虚拟化知识, 例如 DNS 里 A 记录是主机, Cname 是别名，NS 是域名解析服务器。这些比较基本，将不记录在知识点。

EC2

- 从虚拟机内看 Public IP 地址，是 http://169.254.169.254/latest/meta-data/public-ip，但是注意只能看，不是“managed”，不能改。
- EC2 实例类型默认 Default 是共享硬件, Dedicate 和 Host 是独占硬件。Dedicate 和 Host 可以互相切换。
- 创建 EC2 时候可以被赋予一个 IAM Role，这样就无需 KEY 可以直接访问 S3 等系统了。
- 在关闭和终止两种操作下，虚拟机 root 卷上数据会丢失。执行重启实例时候 root 卷的数据不会受到影响。举例如果周五晚关闭了实例周一早再启动，root 卷数据会丢失用户数据变成刚创建的干净的初始镜像。
- 未加密的卷可以生成加密的卷。未加密的快照可以生成加密的快照。
- 已经创建的 Dedicate 实例，只能从 CLI 或者 API 转回到 default 实例。且 VPC 的模式修改了之后，现存的实例依然是 dedicate 模式。需要用 CLI 或 API modify-instance-placement 来调整。调整时候需要关机。
- 竞价实例终止前 2 分钟会发出通知。竞价实例没有 Termination Protection 或者 Delay300 的延迟终止功能。除非：2 分钟内, 正好实例到期, 或者其他原因 AWS 没触发 terminate。否则不管用户看见没看见终止通知，都会 terminate。
- Scheduled Reserved Instances 可以限定预留的时间。
- 如果希望看到底层的 CPU 插槽和 Core 并且买软件参加的授权，则需要 dedicate host 模式。
- EC2 登录的虚拟机时候，public key 在服务器上，private key 在用户端个人电脑上。不能统称为 certificate，应该精确的用名字。

EBS

- EBS 磁盘默认只在本可用区内复制，要想在一个 Region 的多个可用区都复制，那么需要把 EBS 组成 Snapshot（自动存 S3），才可以实现跨多可用区。
- 普通通用型 EBS 最小尺寸是 1GiB，不是 1GB。参考网址。IO 优化型最小 4GB。磁介质最小 500GB。
- EBS 的 Provision IOPS 缩写叫 IO1。每 GB 提供 50 IOPS 保证，最大 64000 IOPS 和 1000MB/s 每个卷。例如容量 4GB，则有 200IOPS。一般创建一个 100GB 的卷，可以有 5000IOPS。参考网址。
- 修改一个已经存在的磁盘的 IOPS，是不断线的，不需要重启虚拟机。
- 需要高性能 IO 的话，实例类型应该也选 EBS 优化实例。
- 吞吐量优化型磁介质（st1）起步 500GB，最大 16TB。吞吐最大 500MB/s。适合大数据、

数据仓库、日志处理，叫做 sequentially 顺序读写。
- 制作快照和恢复快照理论都是瞬间可用。第一次快照可能会比较长。
- 磁盘 IO 是有 Credit 的。如果大部分时间没这么用，短时间爆发一下，则使用 GP2 就可以，不需要专门买 IO1 这种全天候保障 IO 这么贵的场景。
- 已经创建好的卷，不能直接转加密。需要重新创建新卷。

Placement Groups

- 在一个可用区内，Spread 模式一般用于 Hadoop 大数据，一个组最大只能有 7 个实例。
- 如果一个负载有 20 个实例，每个实例都有 500Mbps 的网络流量，这个场景类似是 Hadoop 场景，那么选择将实例分散开，用 Spread 模式更好。如果聚合在一起，反而影响总的吞吐。

EFS

- EFS 的权限管理可以通过 IAM 比较安全。
- EFS 可提供每 1TB 100MB/s 的持续读写性能，参考文档。
- Amazon EFS 在 Windows 实例上不受支持。

AMI

- 复制镜像到别的 Region 时候，Launch Permission、S3 IAM Permission、Tag 等不会被自动复制。因此复制后需要手工配置，再启动。参考文档。
- AMI ID 在不同的 Region 是不一样的。

Storage Gateway

- Gateway-Cache 是以云上为主，缓存本地访问过的数据。
- Gateway-Store 是本地为主，异步同步到云上。
- 客户私有数据中心容量不如，应该用 cache 模式，因为 storage gateway 用 store 模式时候，虽然性能好但是本地需要完全镜像一份，容量放不下。

VPC Network

- Subnet 最小是/28 的网段。
- 总计 5 个预留，前 4 个 IP 预留，0 是网络地址，1 是网关，2 是 DNS，3 是预留。最后 255 是广播地址预留。
- VPC 只能 Peer-to-Peer，不能桥接当做路由器用。不支持 Edge-to-Edge Routing。
- 一个 VPC 只有一个 Internet Gateway。
- 资源创建在同一个可用区内，也可能是随机的分布在多个机房。所以一个可用区的不同 Account 之间传输速度不一样是正常。

- Public subnet 的定义是，有 Internet Gateway 并且至少一条路由从这个 Gateway 出去。
- 新客户的 VPC 在一个 Region 最大只能开 20 个 Instance，VPC 网段只能用/16，要想扩大，开工单申请。
- VPC Endpoint 的作用是让流量不出外网，完全在内网。这个时候要建立的对象是 Interface VPC endpoint。
- 把 EC2 关闭的话，EIP 不会离开 EC2 虚拟机。
- 每次重启 EC2 虚拟机，底层网络“Underlying Host”都会换一个节点，保证 EC2 和原来的节点彻底脱离开。
- Egress-Only Internet Gateways 是有状态的，只用于 IP V6，不能用于 IPV4。

NAT 实例

- NAT 实例和 NAT Gateway 的区别在于，NAT 实例是虚拟机扮演这个角色。
- NAT Instance 是 Net Gateway 之前的做法，可以用一个虚拟机做 NAT，事实上是 Proxy，需要注意网络能力和 CPU 能力，是否能足够带动 500 个 EC2 实例访问外网。NAT Gateway 则是 AWS 自动管理，最大 45Gbps 流量。
- NAT 实例需要配置“禁用源/目标检查”。如果不做这个配置，实例会直接 drop 掉所有流量，不会工作在 forward 转发状态。参考文档。

ELB

- ELB 管理的是 Stateful 的链接，不能 Stateless。
- ELB 只能用于从外网来的流量负载均衡。把 NAT Instance 放在 ELB 里，流量都是出去的方向，ELB 不起作用。
- ELB 入口是一个 public subnet，elb 入口后的 webserver 也是 private zone。为了高可用，一个入口 public subnet 带 2 个 private webzone。所以 1+2=3 是个单数。DB 的 subnet 不计入，因为他是 DB 的 security group 直接生成的。所以就选 3 个。
- 日志可以用来分析收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应等，每 5 分钟发送一次，保存在 S3。为了性能默认不启用日志。不需要 Cloudwatch 来支持日志。
- Application Load Balancer 除支持 7 层的 HTTP/HTTPS 之外，还支持 Websocket 和 HTTP/2 链接。参考网址。
- ELB 健康检查调用的三种方法：Ping、连接检测，某 URL 网页检测。
- ELB 强制客户端要使用 SSL 时候，是依靠“Server Order Preference”来指定。

Security

- 应用于主机的 EC2 的 Security Group 是 Stateful 有状态。
- 应用于 subnet 的 Network ACL 是 Stateless 无状态。
- 默认的 security group 叫做 default，是 allow all 的。如果创建 ec2 时候自己不指定，会会用这个。

- Flow log 可以将 VPC、Subnet 的流量转发给 S3 或 Cloudwatch。其中发到 Cloudwatch 可以直接报警更好。
- 如果要探测 OS 内的非法使用，需要需要装第三方 tools 查看 event 并发送到 Cloudwatch 上。
- 主机上的 EC2 的 Security Group 是 Allow 所有出栈的，除非设置显式的禁止。
- 网络的 Network ACL 默认是进出双向都允许不拦截的。当自定义一个新规则的时候，进出默认都是全拦截，放行也需要手工加入放行策略。
- Network ACL 几乎立刻生效，不需要 take time to propagate。
- AWS Workspace 虚拟桌面产品，传输用的协议是 PCoverIP。
- MFA 双因素认证，使用的是 TOTP（Time-based One Time Password），在 RFC6238 中定义。
- AWS Digital Signature Caculation – Signature Version 4。用的是 V4。
- EMR 产品的安全规则组有点特殊，Master 节点一个组，允许 SSH22 登陆。Slave 节点一个组，只允许和 Master 通信，不允许 SSH。但是这两个组都可以修改。
- 安全规范包括：SOC 1，PCI DSS Level 1，ISO 27001。没有所谓 SOC4 规范。
- AWS 定期做漏洞扫描。客户不能在没有知会 AWS 的情况下做扫描（可能有压力和安全告警）。
- 安全合规的操作方式是：AWS 发布资料给客户并受 NDA 保护。客户不需要就自己的使用再与 AWS 在做沟通，，直接就可以拿 AWS 提供给客户的资料用于合规。
- 安全合规的三要素：人、技术、流程。不含能源（供电）。
- 防 DDoS 的要素是：减少 Internet 入口、减少不信任的暴露、增加非关键部分的出口。扩带宽无用。

Route53

- Route Policy：Simple，延迟，权重，多答案
- 域名解析里边 AAAA 记录是 IPV6 专用。
- 路由策略的英文名字完整版在这里。其中“Default”和“Load Balance”是干扰项清单中没有这种策略。
- R53 的 internal DNS 设计为给 VPC 之内用的，安全规则使的通过 Direct Link 链接的 On premises 的环境访问不了。解决方法：建立一个 EC2，配置为 DNS，使用 Zone 同步，把 dns 同步过来，这个 EC2 可以设置为内外网都可以访问。参考资料。
- 主动-主动故障转移策略，指平时都分配流量。检测到坏的就绕过。主动-被动故障转移策略，平时只给主动分配，除非主动坏掉了才给被动的分配。
- MultiAnswer 是一种既能够同时吐出来多个查询结果，又能自动跳过故障节点的策略。
- PTR 就是传说中的反向解析。
- STP 是在域名商通过 txt 记录，解析出一系列 IP 地址，用于别的邮件服务器识别是否是垃圾邮件。
- Route53 提供两种 zone 场景，1）public zone。2）private zone for VPC。
- 托管别的地方注册的域名的第一步，AWS 希望用户把域名转过来，而不是改 NS 记录。这道题 AWS 认为应该选这个答案。

S3

- S3 也被称为 durable key value store。
- S3 的 Bucket Name 是全球唯一的。
- S3 的两种访问 URL：1）http://s3-aws-region.amazonaws.com/mynewbucket ，2）ttp://mynewbucket.s3-aws-region.amazonaws.com 。
- S3 的文件夹概念是虚拟便于使用的，本身 S3 对象没有文件夹，就是一个个文件。用户设置的文件夹其实是个前缀在文件名最前边。
- S3 的性能可以通过加不同前缀的方式扩展
- S3 Glacier 归档后，检索一般需要 3-5 小时
- 加急检索可以在 1-5 分钟级完成。即所谓“Provisioned expedited retrieval”。加急检索额外收费。
- 多用户授权方式为，再一个 Bucket 下，建立多个目录，分别用 ACL 脚本赋予用户权限。用户从 AD 统一认证。
- S3 的四种加密方式：客户端加密，服务器端 SSE-S3（托管密钥 AES256），SSE-KMS，SSE-C（客户提供密钥）。服务器端有三种，互斥，只能选一个。当访问需要解密时候，需要提供密钥。其中 SSE-S3 是定期自动更新密钥的。SSE-KMS 要通过 KMS 管理密钥。另外的方式每次访问都要管理密钥。
- 当客户提供 envelope 密钥的场景，属于是 SSE-KMS 的加密方式。
- 如果完全不把任何 Key 给用户，者属于 Client 加密，不是三种服务器端加密。只要把 Master 密钥给 AWS，就最少是 SSE-Client 方式。
- 如果要 MUST、ENSURE 客户选择正确的低于，那么一定用地理规则，而不要去押宝全球网络谁的延迟低。
- 删除操作支持 MFA 二次验证。
- 发起一个典型的 PUT 操作，HTTP 头是 Cache-Control、Content-Length、Content-MD5、Content-Type、Expires、x-amz-meta-、x-amz-storage-class 等。这样是 amz 开头，不是 aws 开头。
- 分段上传可以并发执行。分段上传有利于网络抖动和快速恢复，还可以暂停或者继续传。不知道文件大小总体积也可以先上传前边几段。但是不能改进传输安全性。
- 限制 S3 访问的方式：1）S3 Bucket policies、2）Access Control Lists for S3 (Permissions)
- 一致性：read-after-write consistency for PUTS
- 与别人 share 的权限是在 Bucket Policy 里边，而非 CORS 里边。
- 如果一个 EC2 要访问 S3，不应该把 S3 密钥给用户，而是应该创建一个 S3 有权限的 Role，分配给 EC2。
- 读取时候使用 Range HTTP 可以分段获取。
- S3 为了提高读写性能，分拣名可以采用随机字符串开头，例如 16 进制的字符串。
- 要看日志，只要启动 server log 就可以了，不用 cloudwatch。
- 做 global 复制之前，要想打开 version 功能，并在 IAM 中设置对应角色有权限复制。
- S3 的 bucket 权限可以限制的包括：访问者 IP 地址范围，AWS 账户，对象特定前缀。
- 要用 S3 做静态网页存储，要准备的步骤是：1、bucket 与网站名同名。2、设置静态文档 index 和错误页。3、设置文件 public 可见。
- 可以启用 MFA 删除提高安全性。
- 读取到 out-date 的信息是因为正在写入还没完成，所谓的写后读一致性。

Cloudfront

- 静态内容在 S3 全球 CDN 加速，动态内容也可以上 Cloudfront 去加速。
- 支持 Cache Refresh 可以强行刷新文件，每月有一定免费次数。
- Cloudfront 支持的源站包括：1）S3、2）EC2、3）外部其他 IP 地址（近购买 CDN 场景）
- 题目中出现 corporate 的场景都不适合。
- 静态网站(S3)+动态(EC2)混合的网站，要使用的服务是多 Origins 和 Cache Behaviors。OAI 等是给隐私内容用的，多地域是基础功能，任何网站都要用。
- 从 CDN 解析到 ELB，要增加的解析类型是 A 记录，然后在 Alias 下边选 Yes，就能获得 ELB、API gateway 等多种资源。

WAF

- Server IP Log 被占满，使用如下三种：IP Match、Size Constraint Match，String Match。
- 防护应用层：SQL Rejection Match Conditions。

Site-to-Site VPN

- 需要的资源包括：1）A VPC with Hardware VPN Access，2）A Virtual Private Gateway，3）An on-premise Customer Gateway，4）A private subnet in your VPC。参考文档。
- 没有 Virtual Cusomter Gateway 这种概念。Customer Gateway 就是客户侧网关。
- 几种配置示例。

Direct Link

- 开通 Direct Link 后，要从 VPC 上反向发起 ping 私有数据中心，还需要给 VPC 路由表手工写路由，且在 Virtual Private Gateway 上打开路由广播。参考资料。

Fault Tolerance

- Fault tolerance 需要 100%的虚拟机数量，当任何一个可用去挂掉，总虚拟机数量不应该减少。
- 三个区域，如果牺牲一个，另外两个抗起来。此时 Auto-sacling 应该按照 50%标准去扩容。

Auto-scaling

- 每个 Region 默认只能弹起 20 个，更多的需要开 ticket 申请。
- Autoscaling 的工作条件是 Cloudwatch，而不是 ELB。因为有些应用弹起来后就满足条件，不一定要 ELB 来调度。

- Scale-in，缩减时候是策略控制。默认先找实例最多的可用区。然后如果镜像规格不一致，找最老的。如果都是同一个镜像同一个 launch config，找最临近计费周期的。
- 遇到 1 小时内多次扩充和减少，希望能降低频率，则应该调整 Cool down 时间。
- 当和 ELB 联动时候，需要向 Auto Scaling 组添加 Elastic Load Balancing 运行状况检查，否则 ELB 检查不健康的 EC2 不会被 Auto Scalling 替换掉。
- Grace Period 的时间确认是看 1）触发后的冷却期 2）缩减的频繁程度。
- 扩展分为手动扩展、按时间的预定扩展和动态扩展。动态扩展的算法分为目标跟踪扩展、简单扩展和步进（Step）扩展。步进扩展是设置几个阶段，分别是 0~100%，每阶段有不同的扩展策略。各阶段要 100%参数衔接覆盖，不能留有空白区间。
- 弹性组创建时候最少需要提交最小容量和 Launch configuration，其他是可选项。
- 一个 Launch Configuration 最小必填项目是名称、镜像、规格。

AWS Console

- 使用 Resource Group，可以在一个单一页面内管理多种资源。Resource Groups tool, you use a single page to view and manage your resources。参考文档。

CloudWatch

- Cloudwatch 默认看不到 EC2 的内存情况，因为需要装 Agent。由此，CloudWatch 的 Dashboard 默认是没有内存曲线的。
- 监控频率，默认 5 分钟一次。开启 detail 模式，1 分钟一次。参考文档。
- 可以从 EC2 中收集指标，防止 Autoscale 把 EC2 给 terminate 后日志历史无法获取。
- 默认保留 14 天数据。

CloudFormation

- Template 的几大要素，Parameters，Resources，Outputs，不含 Options。
- 配置文件格式：JSON 和 YAML。
- 支持 SQS 等复杂产品。

Elasitc Beanstalk

- 不支持编排 SQS 等复杂产品。只管 app 一层的 EC2 编排。因此需要在使用 CloudFormation 来创建。
- Beanstalk 是编排应用层的，也就是所谓 worker environment。

OpsWork

- 支持的类型包括 Pupput 和 Chef。

RDS

- 可以让应用系统 stateless。
- 题库老的问题，r3.8x.large 目前已经不是最大型号了，可以继续 upgrade 到更大。但题库里边是老的。
- RDS Oracle 限制每个实例 1 个数据库。SQL Server 限制每个实例 100 个数据库。其他 RDS 无限制。
- 创建实例时候，磁盘一样需要选择 gp2 或者 io1 等类型。
- 创建 Aurora，也可以不是多可用区的，因此选择 Aurora 不等于多可用区。
- 创建时候可以选择 RDS 库 encryption，然后 backup 要单独启用 encrption。日志是无法加密的，直接就能看到或下载。
- 创建只读实例后，读写分离需要让业务代码引入带 ro 字样的 endpoint 才能从只读实例读取。
- Aurora 在多个只读实例之间自动负载均衡。
- 默认就是 Provisioned IOPS 格式的硬盘。按容量和 IOPS 计费。
- 不支持 IBM DB2。
- 备份最大保留周期 35 天。
- Aurora 不需要二进制日志来复制数据库集群中的数据或执行时间点恢复 (PITR)。
- SQL Server/Oracle 商业数据库也支持跨 AZ 部署。
- SQL Server/Oracle 商业数据库不支持只读实例。
- SQL Server Enterprise 版本是个特殊版本，因为微软授权协议得关系，只能选择 BYOL，即自带 license，而 AWS 不能提供 license。
- 可以改善 RDS 可用性得是：Snapshot、Read Replica、多 Az。DB Parameters 没有直接帮助。
- 数据库的安全规则组的特点是：默认不打开任何端口，即便是创建 MySQL 默认也不会打开 3306，与 EC2 默认规则组相反。

DynamoDB

- 半结构化数据也适合。
- 时间顺序的分表方式为按时间，每天一个表，旧表的读取 IO Capacity 就变得非常低。
- 分区自动管理，不需要人工干预。
- 可以让应用系统 stateless。
- Value+Data 总计不能超过 400KB。参考文档。
- 数据自动跨 AZ 复制。
- 做强一致性读取的时候，消耗读写单元是最终一致性读取的 2 倍。
- 不用 API 时候，可以走 HTTP 访问。那么需要 DynamoDB Headers attributes。包括 host、content-type、x-amz-date、x-amz-target 等字段。参考文档。
- DynamoDB 能够达到高性能的特点：1）使用 SSD 存储数据，2）自动分区。不包括只读节点和缓存。DynamoDB 界面上没有只读节点配置这种功能。Cache 缓存是 DAX 产品，不是 DynamoDB 产品。
- DynamoDB 的读写是分区的，总的 RCU 和 WCU 一开始均匀分配到所有分区。这时候会收到“ProvisionedThroughputExceededException”的错误。当如果某些区域没有用满，

另外的分区忙碌，系统会自动调高某个区域的限制，让程序继续跑起来。查看设计最佳实践。

- 不能保存结构化数据。
- DynamoDB Auto Scaling 功能可以让系统自动管理读写 capacity，也可以手工调整 WCU 和 RCU。
- Stale Data 不是指近乎归档的老历史数据。Stale Data 是指读取一致性的脏数据。如果老是遇到读取脏数据，那么应该让应用程序用“强一致性读”的方式来房事问 DynamoDB。
- 不适合存大量 CSV。每一个 CSV 是个独立文件，应该考虑 S3。
- DynamoDB 的查询也叫 Query，不叫 search。
- 全局二级索引可以在表建立后再创建。
- 本地二级索引是唯一的，且一旦建立不能修改。
- 一个社交应用有用户名、发帖时间、帖子内容，那么用 DynamoDB 建立表格，分区键选用户名和发帖时间。
- DynamoDB 的加密方式是不支持原生 server-side 自动加密的，因此要加密要么用 client-based，引入 SDK 完成加密，或者用 AWS KMS 机制先加密好，然后写入。

Elastic Cache for Resis

- 可以让应用系统 stateless。
- Redis 是原生的 At-rest 加密。
- 正确使用可以给 RDS 降低查询负载。
- 适合的场景包括：In-Memory Data Store、Gaming Leaderboards (Redis Sorted Sets)、Messaging (Redis Pub/Sub)、Recommendation Data (Redis Hashes)、Other Redis Users。参考文档。
- 启用 Redis Auth 可增加安全性。
- Redis 的一个 Cluster 只有一个节点，1-90 个分片。一个 cluster 可以加只读 5 个副本。
- 安全性通过 IAM 和 Security Group、nACL 实现，没有所谓的 root 密码。
- 如果有一个游戏 APP 有百万人在线，显示评分榜功能最好用 Memcached，因为它支持各种排序。

Elastic Cache for Memcache

- Memcache 加密方式不是原生的 At-rest。而 S3、EBS、EFS 等加密都是 At-rest，Redis 是原生的 At-rest 加密。
- 最大 20 个节点。
- 正确使用可以给 RDS 降低查询负载。
- 集群扩容后，不需要修改程序代码和配置文件。客户端可以使用 auto discovery 功能，能自动使用新扩展出来的节点。

Lambda

- Lambda 访问 RDS 的方式是：1）创建 Lambda 时候，选择 VPC，选择 RDS 已经在的

VPC；2）给 RDS 的安全组放行 Lambda 所使用的安全组。

- 客户业务从单虚拟机膨胀几百倍，看以用 S3 托管静态页，用 Javascript 触发 Lambda，数据库用 DynamoDB，可承受几百倍的压力。
- Lambda 流量外出的时候，可以指定一个 NAT Gateway，然后在 NAT Gateway 上可以绑定 EIP 作为出口 FixIP。
- 使用 AWS Lambda 环境变量操作参数。例如，访问 Amazon S3 时，不应对要写入的存储桶名称进行硬编码，而应将存储桶名称配置为环境变量。
- Lambda 利用 AWS Key Management Service 将敏感信息存储为 Ciphertext，例如保存 RDS 访问账号，以便在 Lambda 函数代码中使用。
- 运行情况需要通过 Cloudwatch 来看。

IAM

- 以下两种认证方式是创建 temporary key 的认证方式：IAM Role，Federation 认证。
- 联合认证的实现方式。先内部 LDAP 认证，再转发 SAML 给 AWS 的 SSO 组件，最后返回 AWS Console。
- Owner 的定义是拥有本账号邮件地址的。
- IAM 上可以建立一个对 S3 有权限的 Role，赋予 EC2 就可以了。
- 给 EC2 赋予一个 IAM Role（含有读写 S3 权限）这个事情，叫做 IAM Instance Profile。
- Lambda 有自己的 VPC 和 SecurityGroup 设置。要访问 VPC 内的资源，需要在对应的 vpc 资源自己的 security group 上，信任 lambda 所使用的 security group。
- Simple AD 是一个可以与 MS AD 兼容的产品，可以简单替代 AD 在 VPC 内用。
- 有一个 IAM 账号只允许有 2 个处于活动状态的（active）可以访问 API 的 Access Key。

KMS

- 关键功能：import your own keys, disable and re-enable keys and define key management roles in IAM are valid。不支持的 Importing keys into a custom key store and migrating keys from the default key store to a custom key store are not possible。HSM 是 CloudHSM 功能，与 KMS 无关。
- AWS KMS Customer Master Keys 是用户管理的主密钥，是不能以未加密的形式离开 KMS 的。用户密钥可以用未加密形式发送出去离开 AWS KMS。
- AWS KMS 用的是信封（Envelop）方式的加密。首先有个 Customer master key（CMK）叫主密钥，然后有一个明文的密钥生成用于加密别的内容。
- 注意 KMS 不是非对称加密（Symmetric）机制，没有 public 和 prviate。题目中 KMS 相关出现这个是错误的。

Billing

- 多个账户可以整合付款。合并享受折扣优惠，独立跟踪各自的使用。
- Linux EC2 是按秒计费，从 2017 年 10 月 2 日起。Windows EC2 是按小时计费，用了 10 分钟关掉，也算 1 小时。再次启动 Windows 实例，要被收取第 2 小时费用。所以 Windows

就别来回开关。

- RI 的三种类型：1）普通预留 RI，2）可转换 RI，3）计划 RI（Schedule）。最常用的 RI 是普通 RI，一次开一年。其次常用的是计划 RI，比如每周六日两天晚上 22 点-2 点运行。
- 竞价示例：如果 Spot 实例在第一个小时内被 Amazon EC2 终止或停止，那么您无需支付使用费。但是如果自己终止了实例，就需要按使用秒数付费。如果 Spot 实例在第一个小时后的任何时间被 Amazon EC2 终止或停止，那么需要按使用秒数付费。如果在 Windows 或 Red Hat Enterprise Linux (RHEL) 上运行并且自己终止了实例，就需要支付一整个小时的费用。
- 利用计划的预留实例（计划实例）主要用于，每日、每周或每月重复一次的容量预留。您应提前预留容量，例如每周六跑特定任务。
- EIP 的收费方式是，买了不用才收费。买了后绑定在资源上，是不额外收费的，因为其实流量已经收费了。买了后如果 EIP 没有被分配到资源，处于闲置状态，那么要额外收费。
- RI 实例买了后是绑定在可用区的。如果希望改 RI，那么 1）可以降低规格，2）可以更换可用区。如果是升级到更高型号，补差价，但对原实例 RI 没有修改。
- EC2 系统盘是不收费的，创建时候选择比 image 默认要大的系统盘也不收费。但是额外加第二块 EBS 会按容量收费。

Amazon Macie

通过机器学习，为数据分类，检测数据的流动，可以做敏感信息防护。

SQS

- 消息包含 ID 和 body 两个元素。目标地点等不是消息的主体。
- 消息有三种状态：1）发布 2）消费 3）删除。当有一个 consumer 来接收消息，进入状态 2 之后，consumer 应该主动删除消息，以防其他 consumer 重复执行。如果一直没删除，则 SQS 会计数 VisibilityTimeout。当到期后，消息对其他 consumer 就变得不可见。最小数据可见期 0，默认 30 秒，最大 12 小时。参考文档。
- SQS 的用法之一：当客户流量快速膨胀，Auto-scaling 来不及响应（需要数分钟）的时候，任务可以在队列里边等着，等忙过来了再处理。至少不会丢失东西。
- FIFO 是保证顺序的，有 IOPS 限制。FIFO 价格与标准队列价格不一最大
- 如果消息不被消费，默认保留 4 天，调整为最大 14 天。
- 消息被消费后，默认可见时间 30 秒。人工可以修改为最大 12 小时。
- 按请求按次计费。一次请求获得大于 64KB 的信息的，每 64KB 大小的消息算一次请求。一般一次请求有 1~10 条消息。总计 256KB。
- 标准队列可承载量很大，但没有顺序保证。没有所谓的工具可以调整顺序。
- 默认是 Short Polling，查询下有无 message 就退出。ReceiveMessage call sets WaitTimeSeconds to 0，或者 ReceiveMessageWaitTimeSeconds=0。可以调整为 Long Polling，设置 ReceiveMessageWaitTimeSeconds 最大是 20 秒。
- 注意：long polling 最大可调整到 20 秒，不是 30 秒。
- Short Polling 查询有无消息就退出，算 1 次请求。如果没查询到浪费请求。Long Polling

可以挂在线上等着消息来，节省请求次数，最高 20 秒超时。

- SQS 可以配置一个 Dead Letter Queue，处理失败的消息就会转到这里。
- 针对 SQS 做 EC2 的弹性扩展时候，可以用 CloudWatch 监控队列内可见消息数量，做为弹性扩容的条件。
- SQS 如果给别的 AWS Account 客户使用，只需要建立 Policy 就可以了，不需要 IAM 设置 Role。

SNS

- SNS 有发布者和订阅者。发布者叫做 Publisher。订阅者主要协议包括：Lambda，SQS，HTTP/S，Email，SMS 这几种。没有其他的如 DynamoDB 这种，没有了。
- SNS 的主题叫做 Topic。
- 一个 SNS 消息，可以 fanout 到两个 SQS 队列，其中一个队列被 EC2 消费做订单处理，另一个可以被 Lambda 调用做大数据分析。
- 如果要大量外发消息，支持的 licent 是 Publisher 和 subscriber client types。
- Fanout 的方式是，建立一个唯一的 SNS topic，然后给好几个 SQS 队列订阅上。
- 支持推送到手机的 Push 服务，需要在对应的平台上创建 Endpoint，然后用这个 enpoint 去订阅 SNS 消息。
- Topic 被删除后，要重新建立同名的 topic 需要 30-60 秒的缓冲时间，等以前的都消费完了才可以创建。
- 消息一旦被 publish 到 topic 后，是不能召回 Recall 的，没有所谓“recall parameters“。

SWF

- SWF 的作用是 keeps track of all tasks and events。
- 如果要确认一个系统的消息不会被消费多余一次，必须同步或者异步完成，并且是由一个逻辑的决策人来确认是否执行完成了。这个场景最佳是用 SWF。
- 开始启动一个 task 的操作叫做”Workflow starter”，后续操作者叫“Activity Starter“。每个步骤的确认者都是”Decider“。参考文档。
- 一个公司的一系列业务，应该在一个 domain 下创建多个 workflow。这样 workflow 之间可以互动。如果是多个 domain，就不能互动了。
- 推动流程进展的 actor 可以有多种类型，例如 Workflow Starter，Activity Worker，Decider。

Trust Advisor

- 支持从成本、性能、安全、高可用、服务限制五个方面做建议。
- 不提供反病毒扫描、安全漏洞扫描等。

Support

- 付费客户响应时间： General guidance 1 天； System impaired 12 小时； 商业计划客户生产系统受损 4 天；生产系统停机 1 小时。企业计划客户 Business-critical system down15

分钟。

Compliance

- 客户可以节约一部分费用。不可以让客户来 AWS Site 考察。已经在用 AWS 的服务的部分，可以不用在申请证书了，AWS 会提供证书的复印件。
- AWS 通过 PCI DSS，但是客户自己的业务系统要想保存信用卡信息，还需要客户自己去 QSA 申请证书。参考文档。

AWS Config

- Analyze 账户库存并监控流程的变更
- Config 用来做类似 CMDB 和资产管理的追踪和审计，例如 access to historical configurations of your resources to evaluate relevant configuration change。

Redshift

- 一般用于数据仓库，MPP 方式的分布式，适合以后数百 TB 量级的结构化数据增长。
- 对比：Aurora 最大只有 64TB。
- 数据容灾复制场景，可以将一个已经存在的库 SPAN 到两个 region。
- 如果是全新是 Create，则启动集群时候可以加密。如果一开始没有加密，后续可以配置“AWS KMS”启用加密。配置后，原集群会自动加密，加密的集群创建的快照也是加密的。加密的集群也可以返回未加密的集群。参考文档。
- Redshift 加密是四层加密，分别是：主密钥、集群密钥、数据库密钥、数据加密。

Amazon Kinesis Data Streams

- 与 SQS 的区别：Kinesis 适合类型为 Event 的处理，例如收集海量日志。适合并行使用同一个数据流。实时处理。排序。7 天内按顺序回放。单个数据包 1MB。
- Kinesis 适合处理网站点击、物联网等。可以排序，可以直接分析比 SQS 适合收集 1 秒 50000 次点击提交的场景。
- SQS 适合语义消息，每个报文单独跟踪，实现应用内部多个模块间解耦，延迟 15 分钟投递，可允许流量扩展。
- UpdateShardCount 可以增加处理能力

AWS Systems Manager Parameter Store

- 支持 Lambda 的密钥管理，例如 Lambda 访问 RDS 等。
- 目前不支持 S3

Cloudtrail

- Cloudtrail 做 API 的审计，是一次创建一个规则，apply 到所有 region。

Organization

- 为员工屏蔽掉一些服务的方法，可以通过 Organization 服务进行。添加一个 OU，再配置策略，就可以为下属员工账号屏蔽不想提供的服务。

Private Link

- 设计个人身份信息（PII）的数据进入 Internet，对 HIPAA 或 PCI 等法规的合规性，可使用 PrivateLink，将 VPC 内的多种服务资源保护起来。

Data Pipeline

- 一项数据管理和导入的工具，支持 EC2、EMR 转换，支持 DynamoDB、RDS、Redshift、S3 做存储。

Snowball

- Snowball 在安全上属于 Data at transit，是因为他的目标是运输数据。不算是 Data at rest。