## EC2

### 问：我应该选择哪种卷？

现在，客户可在 3 种 EBS 卷类型间选择满足其工作负载所需的卷类型，即：通用 (SSD)、预配置 IOPS (SSD) 和磁性介质。通用型 (SSD) 是一款以 SSD 为支持的全新通用型 EBS 卷类型，也是我们推荐给客户的默认类型。通用型 (SSD) 卷适用于各种工作负载，包括小型到中型数据库、开发和测试环境以及启动卷。预配置 IOPS (SSD) 卷提供的存储具有一致性高和延迟低的特点，旨在为 I/O 密集型应用程序提供服务，例如大型关系数据库或 [NoSQL 数据库。](https://aws.amazon.com/cn/nosql/)与其他 EBS 卷类型相比，磁性介质卷可提供最低的每 GB 成本。对于数据不常被访问的工作负载以及看重低存储成本的应用来说，磁性介质卷是理想的选择。

### 问：是否可以使用常规的 Amazon S3 API 访问我的快照？

否，只能通过 Amazon EC2 API 访问快照。

### 问：如果停用某个 Amazon EC2 实例的监控，是否会丢失指标数据？

您可以接收自开始监控 Amazon EC2 实例起最多 2 周时间内的指标数据。两周后，如果已停用了 Amazon EC2 实例的监控，则该 Amazon EC2 实例的指标数据将不可用。如果要存档 2 周以上的指标，您可以从命令行中调用 mon-get-stats 命令，并在 Amazon S3 或 Amazon SimpleDB 中存储结果。

### 问：当在我 5 分钟和 1 分钟时段内查看时，为什么同一时间窗口的图形会有不同？

如果在 5 分钟和 1 分钟时段内查看同一时间窗口，您可能会发现数据点显示在图形中不同的位置上。对于您在图形中指定的时段，Amazon CloudWatch 会查找所有可用的数据点，再计算出单个聚合点来代表整个时段。在 5 分钟时段的情况下，该单一数据点会处于 5 分钟时间窗口的开头。在 1 分钟时段的情况下，该单一数据点会处于 1 分钟标记上。我们建议使用 1 分钟周期来进行故障诊断，以及其他要求最精确的时段图形的活动。

### 问：是否可以快速扩展但缓慢缩小我的 Amazon EC2 容量？

可以。例如，您可以定义一个增大条件，将 Amazon EC2 容量增加 10%，再定义一个缩小条件，将其容量缩小 5%。

### 问：如果删除 Auto Scaling 组，我的 Amazon EC2 实例会发生什么情况？

如果您的 Auto Scaling 组中有运行的实例，而且您选择删除该 Auto Scaling 组，则实例会被终止，Auto Scaling 组会被删除。

### 问：Elastic Load Balancing 支持哪些协议？

Elastic Load Balancing 支持对使用 HTTP、HTTPS（安全 HTTP）、SSL（安全 TCP）和 TCP 协议的应用程序执行负载均衡。

### 问：可以为哪些 TCP 端口执行负载均衡？

您可以为下列 TCP 端口执行负载均衡：

* [EC2-VPC] 1-65535
* [EC2-Classic] 25、80、443、465、587、1024-65535

### 问：我想从预留实例市场中的第三方卖家处购买低和/或中使用率预留实例。这些实例与无预付、部分预付和全额预付预留实例之间有何区别？

上一代预留实例与当前一代预留实例在成本节约方面具有相同的优势。不同之处在于每小时成本的计算方式。

* **低使用率预留实例**：这些实例提供最低的预付款要求。除了预付款较低之外，每小时的使用费也可以享受大幅折 扣。低使用率预留实例允许您随时关闭按需实例，而不支付按小时使用费。对于存在零星使用需求的实例（如每天运行约 7-12 个小时的开发和测试实例）或用于短期项目且每年运行 3-7 个月的实例而言，这些低使用率预留实例是理想之选。
* **中等使用率预留实例**：这些实例的预付款比低使用率预留实例高，但按小时使用费相对较低。中使用率预留实例允许您随时关闭按需实例，而不支付按小时使用费。它们最适用于在大多数时间运行、但使用情况会发生一些变化的工作负载。

上一代预留实例仅在第三方卖家的预留实例市场中提供，并且各个实例的运行期限不同。

### 问：能否将预留实例从一个实例类型（例如 c1.xlarge）重新分配到另一个实例类型（例如 m1.large）？

不能。预留实例在其运行期限内与特定实例类型相关联；然而，如果该实例为 Linux/UNIX 预留实例，您可以从一种实例大小（例如 c3.large）更改为同一类型中的另一种实例大小（例如 c3.xlarge）。

### 问：竞价型实例与按需实例或预留实例有何区别？

竞价型实例可以让客户无需预付即可购买计算容量，其小时费率也通常低于按需实例的费率。通过竞价型实例，您可以指定愿意为运行 某特定实例类型支付的最高小时单价。Amazon EC2 为各个可用区的每一实例类型设置一个现货价格，该价格是所有客户在给定期间运行竞价型实例而支付的小时单价。现货价格会随着实例的供需而浮动，但客户支付 的价格不会超过他们所指定的最高价格。如果现货价格超过客户的最高价格，Amazon EC2 将关闭该客户的实例。除了这些区别以外，竞价型实例与按需实例或预留实例的运行是完全相同的。有关竞价实例的详细信息，请参阅[此处](https://aws.amazon.com/cn/ec2/purchasing-options/spot-instances/)。

### 问：如果 Amazon EC2 在未满一小时前终止了我的竞价型实例，是否依然向我收取费用？

不会。如果竞价型实例是由 Amazon EC2 终止的，则您无需支付未满一小时的使用费。不过，如果是您自己终止了实例，则该实例所运行的任何时间您都需要付费。

### 问：我能否将竞价型队列与 Elastic Load Balancing、Auto Scaling 或 Elastic MapReduce 配合使用？

不能，Elastic Load Balancing、Auto Scaling 或 Elastic MapReduce 不能直接触发竞价型队列请求。

### 问：微型实例可以提供多少计算能力？

微型实例提供少量持续的 CPU 资源，但您可用其他周期在短时间内将 CPU 容量突增至 2 个 ECU。 它们非常适合具备下述特点的较低吞吐量应用程序和网站：定期消耗大量的计算周期，但在其他时间中只消耗极少的 CPU 来用于后台进程和守护程序等。[详细了解](http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/concepts_micro_instances.html)如何将使用此类实例。

### 问：微型实例与标准小型实例相比，在计算能力上有何不同？

在稳定状态时，微型实例接收的计算资源仅占小型实例所能接收的一小部分。因此，如果您的应用程序具有计算密集型或稳定状态需 求，我们建议您使用小型实例（或者依据您的需求，使用更大型的实例）。然而，微型实例可以定期突增至多达 2 个 ECU（短时间内）。这是标准小型实例可用的 ECU 数的两倍。因此，如果您有相对较低吞吐量的应用程序或网站，并且偶尔需要消耗大量的计算周期，则建议您使用微型实例。

### 问：计算优化实例应该何时使用？

计算优化实例经过专门设计，适用于可从高计算能力中受益的应用程序。这类应用程序包括：高性能前端集群、Web 服务器、批量处理、分布式分析、高性能科学和工程应用、广告服务、MMO 游戏、视频编码和分布式分析。

### 问：我应该何时使用 GPU 实例？

GPU 实例最适用于并行度极高的应用程序，例如，使用数千个线程的工作负载。例如，图形处理有大量的计算要求，其中的每个任务都相对较小，执行的一组操作形成了 一个管道，而此管道的吞吐量要比单个操作的延迟更为重要。要构建能充分利用这种并行度的应用程序，用户需要掌握 GPU 设备的专项知识，了解如何针对各种图形 API（DirectX、OpenGL）或 GPU 计算编程模型（CUDA、OpenCL）进行编程。

### 问：G2 实例与 CG1 实例有何不同？

CG1 实例使用 NVIDIA Tesla GPU，设计用于使用 CUDA 或 OpenCL 编程模型进行的一般 GPU 计算。CG1 实例为客户提供了高带宽 10Gbps 网络、双精度浮点功能以及纠错代码 (ECC) 内存，因此非常适用于高性能计算 (HPC) 应用程序。G2 实例使用 NVIDIA GRID GPU，可为使用 DirectX 或 OpenGL 的图形应用程序提供一个经济实惠的高性能平台。NVIDIA GRID GPU 还支持 NVIDIA 的快速捕获和编码 API。示例应用程序包括视频创建服务、3D 可视化、流图形密集型应用程序以及其他需要大量并行处理能力的服务器端工作负载。另外，图形实例还可用于使用 CUDA 或 OpenCL 进行的一般计算，但不建议用于网络密集型 HPC 应用程序。

### 问：什么是集群计算实例？

集群计算实例将高计算资源和高性能联网两者相结合，适合高性能计算 (HPC) 应用程序和其他高要求的网络绑定型应用程序。集群计算实例提供与其他 Amazon EC2 实例相似的功能，但经过了专门设计，能够提供高性能联网功能。

用户可以通过 Amazon EC2 集群置放群组功能将集群计算实例分组到集群中，让应用程序获得紧密耦合节点对节点通信（许多 HPC 应用程序的典型特征）所需的低延迟网络性能。集群计算实例还可大幅提升 Amazon EC2 环境内以及至 Internet 的网络吞吐量。因此，这些实例也非常适合需要执行网络密集型操作的客户应用程序。

### 问：在集群置放群组中启动实例时有望实现哪些网络性能？

EC2 实例在集群置放群组中可利用的带宽取决于实例类型及其联网性能规格。在置放群组中启动精选的 EC2 实例时，这些实例可使用高达 10Gbps 的单流流量和 20Gbps 的多流流量（全双工）。集群置放群组之外（例如，发送至 Internet）的网络流量被限制在 5Gbps（全双工）。

### 问：什么是集群置放群组？

集群置放群组是一种逻辑实体，可以通过作为组的一部分启动实例来创建实例集群。然后实例集群就能在该组的实例之间提供低延迟、全等分的 10 Gbit 以太网带宽连接。您可以通过 Amazon EC2 API 或 AWS 管理控制台创建集群置放群组。

### 问：高 I/O 实例是什么？

高 I/O 实例使用基于 SSD 的本地实例存储，为应用程序提供极高的低延迟性和 I/O 容量，最适合需要数万 IOPS 的应用程序。与集群实例相似，高 I/O 实例可以通过集群置放群组进行集群化，实现高带宽联网功能。

### 问：hi1.4xlarge 实例的连续吞吐量为多少？

所有 AMI 类型 （Linux PV、Linux HVM 和 Windows） 上的连续吞吐量为大约 2GB/s 读取和 1.1GB/s 写入。

### 问：突发性能实例有什么与众不同？

Amazon EC2 允许在固定性能实例（例如 M3、C3 和 R3）和突发性能实例（例如 T2）之间进行选择。突发性能实例为 CPU 性能提供基本水平的同时具有短期发挥更高性能的能力。T2 实例适用于不会经常（或始终）用尽 CPU 性能但偶尔需要突发性能的工作负载。

T2 实例的基本性能和突发能力受到 CPU 积分的制约。每个 T2 实例都会持续收到 CPU 积分，其频率取决于实例大小。T2 实例会在其空闲时累计 CPU 积分，然后在活跃时使用 CPU 积分。一个 CPU 积分可以在一分钟内提供完整的 CPU 核心性能。下表显示了每个 T2 实例大小的最大积分余额和基本性能。当突增至全核心性能时，T2 实例的每个 vCPU 能以每小时 60 分的最大速度消费 CPU 积分。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **型号** | **vCPU** | **CPU 积分/小时** | **最大 CPU 积分余额** | **基本 CPU 性能** |
| **t2.nano** | 1 | 3 | 72 | 一个内核的 5% |
| **t2.micro** | 1 | 6 | 144 | 一个内核的 10% |
| **t2.small** | 1 | 12 | 288 | 一个内核的 20% |
| **t2.medium** | 2 | 24 | 576 | 一个内核的 40%\* |
| **t2.large** | 2 | 36 | 864 | 一个内核的 60%\*\* |

*\* 对于 t2.medium，单线程应用程序可以使用 1 个内核的 40%；如果需要，多线程应用程序可以使用两个内核，各用 20%。*

*\* 对于 t2.large，单线程应用程序可以使用 1 个内核的 60%；如果需要，多线程应用程序可以使用两个内核，各用 30%。*

例如，t2.small 实例以每小时 12 个 CPU 积分的频率持续接收积分。这项功能提供的基本性能相当于 CPU 核心的 20%。当实例不需要其所接收的积分时，会将积分储存在 CPU 积分余额中，保留 24 小时。当 t2.small 需要超过核心 20% 的突发性能时，会从 CPU 积分余额中将其取出使用，以无缝应对突发的性能需求。经过一段时间后，如果您发现工作负载需要消费您更多的 CPU 积分，或者实例的 CPU 积分余额不足，建议您选择更大的 T2 实例，例如 t2.medium 或固定性能实例类型。

许多应用程序（例如 Web 服务器、开发人员环境和小型数据库）不需要 CPU 持续高速运行，但是需要在适当的时候让 CPU 运行在非常高的速度上。T2 实例正是针对这类使用情况而专门设计的。对于像视频编码、高容量网站或 HPC 应用程序这类需要持续 CPU 高性能的应用，我们建议您使用固定性能实例。T2 实例的设计理念是在应用确实需要 CPU 性能时提供媲美专用高速 Intel 内核的性能，同时避免其他环境中因为过度订购而可能经常出现的性能波动或其他常见的不良作用

### 问：什么是密集存储实例？

密集存储实例专用于需要对超大型数据集合进行高速的连续读写访问的工作负载，例如 Hadoop 分布式计算、大规模并行处理数据仓库以及日志处理应用程序。与其他 EC2 实例相比，密集存储实例提供了最佳的 GB 存储价格比和磁盘吞吐量价格比。

问：何时应使用内存优化型实例？  
内存优化型实例可为内存密集型应用程序（包括内存中应用程序、内存中数据库、内存中分析解决方案、高性能计算 (HPC)、科学计算以及其他内存密集型应用程序）提供大容量内存。

### 问：使用 VM Import/Export 导出 EC2 实例是否有任何其他要求？

对于之前用 VM Import/Export 导入的 EC2 实例，您可以导出正在运行或已停止的实例。如果实例正在运行中，它会暂时停止以便为引导卷拍摄快照。无法导出 EBS 数据卷。无法导出具有多个网络接口的 EC2 实例。

### 问：是否可以导出连接了一个或多个 EBS 数据卷的 Amazon EC2 实例？

可以。但是 VM Import/Export 仅导出 EC2 实例的引导卷。

### 问：导入虚拟机有什么费用？

上传和存储虚拟机映像文件时，您需要支付标准的 Amazon S3 数据传输和存储费。导入虚拟机后，则适用标准的 Amazon EC2 实例小时费和 EBS 服务费。如果导入过程完成后您不再希望将 VM 映像文件存储在 S3 中，请使用 ec2-delete-disk-image 命令行工具从 Amazon S3 删除您的磁盘映像。

### 问：导出虚拟机有什么费用？

您需要支付标准的 Amazon S3 存储费，以存储您导出的 VM 映像文件。在将导出的 VM 映像文件下载到内部虚拟环境中时，您还要支付标准的 S3 数据传输费。最后，您要支付标准的 EBS 费用，以存储 EC2 实例的临时快照。为了尽可能降低存储费用，请在 VM 映像文件下载到您的虚拟环境中后，将其从 S3 中删除。

### 问：导入 Windows Server 2003 或 2008 的虚拟机时，操作系统许可由谁负责提供？

在启动使用 Microsoft Windows Server 2003 或 2008 的已导入 VM 时，您需支付标准的实例小时费，以便 Amazon EC2 运行相应的 Windows Server 版本，这其中包含了在 Amazon EC2 中使用该操作系统的权限。您需负责确保所有已安装的其他软件具有适当的许可。

那么，在导入 Windows Server 2003 或 2008 的 VM 后，我内部的 Microsoft Windows 许可密钥会出现什么情况？在作为 EC2 实例运行您导入的 VM 时，不会使用之前与该 VM 关联的内部 Microsoft Windows 许可密钥，因此您可以将该密钥重复用于内部虚拟环境中的其他 VM。

### 问：将 EC2 实例导回到我的内部虚拟环境后，是否可以继续使用 AWS 提供的 Microsoft Windows 许可密钥？

不可以。导出 EC2 实例后，该 EC2 实例中使用的许可密钥便不再可用。在内部虚拟平台中启动导出的 VM 后，您将需要重新激活并指定新的许可密钥。

### 问：Amazon EC2 服务等级协议有什么保证？

我们的 SLA 保证在某一区域内，Amazon EC2 和 Amazon EBS 的月度正常运行时间百分比至少为 99.95%。

## Dynamodb

### 问：Amazon DynamoDB 可以代我进行哪些管理？

Amazon DynamoDB 消除了影响数据库扩展的主要绊脚石之一，即数据库软件的管理，以及运行数据库所需的硬件配置。客户可在短短几分钟之内部署非关系数据库。当表大小增大或您 增加配置吞吐量时，DynamoDB 可自动对您的数据进行分区和再分区，并配置额外的服务器容量。此外，Amazon DynamoDB 还可在 AWS 区域的三个设施上同步复制数据，为您提供数据高可用性和数据持久性。

### 问：为什么 Amazon DynamoDB 是基于固态硬盘构建的？

Amazon DynamoDB 完全运行在固态硬盘 (SSD) 上。SSD 有助于我们实现设计目标，即在可预测的低延迟响应时间之内，存储和访问任何规模的数据。SSD 还具有很高的 I/O 性能，使我们能够经济高效地处理大规模请求工作负载，并能将这种成本效益以较低的请求价格让渡给客户。

### 问：DynamoDB 的存储成本似乎很高。对我的使用案例来说，这项服务划算吗？

和任何其他产品一样，我们建议 Amazon DynamoDB 的潜在客户考虑解决方案的整体成本，而不要只局限于单个价格指标。处理数据库工作负载的总成本受到两个因素的影响：请求流量要求、存储的数据量。大部分数 据库工作负载的特点是，每存储 1GB 数据都需要很高的 I/O（每秒读取次数和每秒写入次数很高）。Amazon DynamoDB 是基于 SSD 驱动器构建的，相对于旋转介质而言，它每存储 1GB 数据的成本有所提高，但让我们能够提供非常低的请求成本。根据我们在典型数据库工作负载方面的经验，我们认为，相较于使用典型的基于旋转介质的关系数据库 或非关系数据库，使用基于 SSD 的 DynamoDB 服务的总费用通常更低。如果您的使用案例需要存储大量数据，但这些数据的访问频率很低，则 DynamoDB 可能不太适合您。对于此类使用案例，我们建议您使用 S3。

同时还应注意，存储成本反映了将每个数据项的多个副本存储于同一 AWS 区域内多个设施的成本。

### 问：DynamoDB 支持哪种类型的查询功能？

Amazon DynamoDB 支持使用用户定义的主键来执行 GET/PUT 操作。主键是表中项目仅有的一个必需属性，并且唯一地标识每个项目。您在创建表时指定主键。除此之外，DynamoDB 还支持您使用全局二级索引和本地二级索引对非主键属性进行查询，从而提供灵活的查询服务。

主键可以是单属性的分区键或复合的分区-排序键。例如，单属性的分区主键可以是“UserID”。这使您能够快速读取和写入与特定用户 ID 相关联的项目的数据。

复合的分区-排序键可作为一个分区键元素和一个排序键元素进行索引。这个多部分键可保持第一个元素值和第二个元素值之间的层次 结构。例如，复合的分区-排序键可以由“UserID”（分区）和“Timestamp”（排序）组成。通过保持分区键元素的恒定，您可以在排序键元素中 进行搜索以检索项目。这样您就可以使用 Query API 进行检索，例如在一系列时间戳中检索带有单个 UserID 的所有项目。

想要了解更多有关全局二级索引及其查询功能的信息，请参阅常见问题中的“[二级索引](https://aws.amazon.com/cn/dynamodb/faqs/#gsi_anchor)”部分。

### 问：什么时候应该使用 Amazon DynamoDB，而不是使用 Amazon RDS 或 Amazon EC2 上的关系数据库引擎？

当今基于 Web 的应用会生成和消耗大量数据。例如，某个在线游戏刚推出时可能只有几千个用户，数据库工作负载很小，每秒进行 10 次写入和 50 次读取操作。但是，如果游戏取得成功，则可能很快会发展到拥有数百万个用户，读写操作次数达到每秒数万次甚至每秒数十万次。每天可能生成数 TB 甚至更多数据。利用 Amazon DynamoDB 开发应用程序，您能够从较小规模起步，随着要求的提高而增加表的请求容量，同时不会发生停机。您只需为您配置的请求容量支付低廉的费用，并让 Amazon DynamoDB 在足够的服务器容量上执行数据和流量分区工作，从而满足您的需求。将数据库管理的工作交给 Amazon DynamoDB 来打理，您只需要存储和请求数据即可。自动复制和故障转移功能实现了内置容错、高可用性和数据持久性。Amazon DynamoDB 确保您的数据库得到全面管理，并可随着应用程序要求的提高而扩展，令您高枕无忧。

尽管 Amazon DynamoDB 解决了数据库可扩展性、管理、性能和可靠性等核心问题，但它并不具备关系数据库的全部功能。它不支持复杂关系查询（例如联接）或复杂事务。如果您的工作负 载需要此功能，或者您寻求与现有关系引擎实现兼容，则您可能需要在 Amazon RDS 或 Amazon EC2 上运行关系引擎。虽然关系数据库提供稳健的特性和功能，但要在单个关系数据库实例的基础上扩展工作负载是非常复杂的，而且需要大量的时间和专业知识。因 此，如果您预计到新应用程序的扩展要求，而且不需要使用关系功能，则 Amazon DynamoDB 可能是您的最佳选择。

### 问：什么时候应该使用 Amazon DynamoDB，而不是使用 Amazon S3？

Amazon DynamoDB 存储按主键索引的结构化数据，实现对从 1 字节到 400KB 的项目的低延迟读取和写入访问。Amazon S3 存储非结构化 Blob，适合存储最大 5 TB 的大型数据元。为了优化您使用 AWS 服务的成本，应将大型数据元或不常访问的数据集存储在 Amazon S3 中，而最好将小型数据元素或文件指针（可能指向 Amazon S3 对象）保存在 Amazon DynamoDB 中。

### 问：数据模型是什么样的？

Amazon DynamoDB 的数据模型如下：

表：表是数据项的集合 – 就好比关系数据库中的表是行的集合。每个表具有无限数量的数据项。Amazon DynamoDB 是无架构的，因为表中的数据项不必具有相同的属性，甚至不必具有相同数量的属性。每个表必须具有一个主键。主键可以是单个属性键，也可以是组合了两个属性 的“复合”属性键。每个项目都必须具有您指定为主键的属性，因为主键对表中的各个项目进行唯一标识。

项目：项目包括一个主键或复合键，以及数量不限的属性。与单个项目相关联的属性数量没有明确限制，但项目的总大小（包括所有属性名称和属性值）不得超过 400KB。

属性：与数据项相关联的每个属性包括属性名称（例如“Color”）以及一个值或一组值（例如“Red”或“Red、Yellow、Green”）。单个属性没有明确大小限制，但项目的总大小（包括所有属性名称和值）不得超过 400KB。

### 问：什么是扫描操作的一致模型？

答：扫描操作支持最终一致性读取和一致性读取。默认情况下，扫描操作具有最终一致性。不过，您可以在 Scan API 调用中使用可选的 ConsistentRead 参数，修改一致性模型。将 ConsistentRead 参数设为 true 后，您可以通过扫描操作进行一致性读取。有关详细信息，请参阅扫描操作的相关[文档](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_Scan.html)。

### 问：单个表的吞吐量是否有限制？

没有限制。您可以使用 UpdateTable API 或在 AWS 管理控制台中增加为表配置的吞吐量。DynamoDB 能够大容量运行，您可以达到的最大吞吐量没有理论上的限制。DynamoDB 自动将表分为多个分区，其中每个分区都是一个独立的并行计算单元。DynamoDB 可以通过添加更多分区，不断提高吞吐率。

如果您希望吞吐率超过每秒 10000 次写入或每秒 10000 次读取，请首先[填写此在线表格与 Amazon 联系](http://portal.aws.amazon.com/gp/aws/html-forms-controller/DynamoDB_Limit_Increase_Form)。

### 问：什么是全局二级索引？

全局二级索引是包含不同于表的主键的分区键或分区-和-排序键的索引。

为对表中的数据进行高效访问，Amazon DynamoDB 针对主键属性创建并维护其索引。这可以让应用程序通过指定主键值快速地检索数据。但是，包含一个或多个二级（或替代）键也能使许多应用程序受益，因为这可 以让它们更高效地访问其属性与主键不同的数据。要实现这一目的，您可以在表中创建一个或多个二级索引，并对这些索引发出 Query 请求。

Amazon DynamoDB 支持两种类型的二级索引：

* 本地二级索引 – 分区键与表相同但排序键不同的索引。本地二级索引之所以称为“本地”，是因为该索引的每个分区的范围都限定为具有相同分区键的表分区。
* 全局二级索引 – 分区键或分区-和-排序键可与表中的这些键不同的索引。全局二级索引之所以称为“全局”，这是因为该索引上的查询可跨过所有分区，涵盖表中的所有项目。

二级索引由 Amazon DynamoDB 以稀疏数据元的形式自动维护。只有当项目存在于定义索引所引用的表中，它们才会出现在索引中。这使得按索引进行查询变得非常高效，因为索引中的项目数通常远远少于表中的项目数。

全局二级索引支持非唯一属性，它允许在表中按任何非键属性进行查询，从而提高了查询的灵活性。

比如说，某个游戏应用程序将玩家信息存储在 DynamoDB 表中，该表的主键由 *UserId*（分区）和 *GameTitle*（排序）组成。项目中包含名称为 *TopScore*、*Timestamp*、*ZipCode* 的属性，以及其他一些属性。创建表以后，DynamoDB 在主键上提供隐式索引（主索引），以便能够高效地查询并返回某个特定用户在所有游戏中获得的最高分。

但是，如果应用程序需要获得用户在某个特定游戏中的最高分，则使用这种主索引查询的效率极低，并且需要在整个表中进行扫描。反之，以 GameTitle 为分区键元素并以 TopScore 为排序键元素的全局二级索引能让应用程序快速检索某个游戏的最高分。

GSI 不需要排序键元素。例如，您的 GSI 可以拥有一个只带分区元素 *GameTitle* 的键。在以下示例中，GSI 没有投影属性，因此它只会返回属性与您正在查询的 *GameTitle* 相匹配的所有项目（通过主键识别）。

### 问：全局二级索引应该在什么时候使用？

全局二级索引尤其适用于追踪具有很多不同值的属性之间的关系。例如，您可以创建 DynamoDB 表并将 *CustomerID* 用作该表的主分区键，将 *ZipCode* 用作全局二级索引的分区键，因为邮政编码的数量很多，而且您可能会拥有很多客户。使用主键，您可以快速获得任何客户的相关记录。使用全局二级索引，您可以高效查询居住在指定邮政编码地区的所有客户。

### 问：全局二级索引与本地二级索引有何不同？

全局二级索引和本地二级索引都能提高查询的灵活性。[LSI](https://aws.amazon.com/cn/dynamodb/faqs/#lsi_anchor) 与特定的分区键值相关联，而 GSI 则可以涵盖所有的分区键值。由于具有相同分区键值的项目在 DynamoDB 中共享同一分区，所以“本地”二级索引只包含存储在同一位置（相同分区）的项目。因此，LSI 可用于查询分区键值相同但排序键值不同的项目。例如，假设有某个用于追踪客户订单的 DynamoDB 表，其中 *CustomerId* 为分区键。

在 *OrderTime* 上建立的 LSI 可以高效地查询并检索出特定客户最近订购的产品。

相比之下，GSI 并不局限于具有共用分区键值的项目。相反，GSI 与主键一样，可以跨越表的所有项目。在上表中，在 *ProductId* 上建立的 GSI 可用于高效地查找特定产品的全部订单。请注意，本示例中没有指定 GSI 排序键，即使可能有很多订单的 *ProductId* 相同，它们也将作为单独的项目存储在 GSI 中。

为了确保表和索引中的数据共处于同一个分区，LSI 将每个分区键值的全部元素（表和索引）的总大小限制为 10GB。GSI 不强行要求数据共处，且不做任何此类限制。

当您向表中写入内容时，DynamoDB 自动更新所有受影响的 LSI。相反地，对于表中定义的任何 GSI 进行的更新最终会保持一致。

LSI 允许 [Query API](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_Query.html) 检索投影列表之外的属性。这不是 GSI 支持的行为。

### 问：全局二级索引是如何工作的？

GSI 的行为方式在许多方面与 DynamoDB 表相似。您可以使用 GSI 的分区键元素查询 GSI，同时对排序键元素使用条件筛选器。然而，两者又有不同，DynamoDB 表的[主键](http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DataModel.html#DataModelPrimaryKey)必 须是唯一的，而 GSI 键可以由多个项目共用一个。如果存在具有同一 GSI 键的多个项目，则将按单独的 GSI 项目对其进行追踪，并且 GSI 查询会将它们作为单独的项目全部检索出来。当增加、删除或更新项目时，DynamoDB 会在内部确保 GSI 的内容得到相应地更新。

DynamoDB 将 GSI 的投影属性存储在 GSI 数据结构中，同时还存储了 GSI 键和匹配项目的主键。GSI 使用源表中的投影项目的存储。这可以确保根据 GSI 而不是表进行查询，从而提高查询的灵活性并改进工作负载的分配。因此，查询 GSI 索引不会返回：属于表中项目的一部分，但不属于 GSI 键的属性、该表的主键以及投影属性。如果应用程序需要在查询 GSI 后从表中获得其他数据，则可从 GSI 中检索主键，然后使用 [GetItem](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_GetItem.html) 或 [BatchGetItem](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_BatchGetItem.html) API 从表中检索需要的属性。由于 GSI 具有最终一致性，所以使用此模式的应用程序必须要考虑在 GSI 和 GetItem/BatchItem 调用期间项目被删除（从表中删除）的问题。

当对表进行相应更改时，DynamoDB 将自动处理 GSI 中的项目增加、更新和删除。将某个项目（具有 GSI 键属性）添加到表中时，DynamoDB 会对 GSI 进行异步更新，以增加此新项目。同样地，将某个项目从表中删除时，DynamoDB 会从受影响的 GSI 中删除该项目。

### 问：是否可以为基于分区的表和分区-排序结构表创建全局二级索引？

可以，无论 DynamoDB 表拥有何种类型的主键，您都可以创建全局二级索引。该表的主键可能只包括一个分区键，也可能同时包括分区键和排序键。

### 问：全局二级索引的一致性模型是什么？

GSI 支持最终一致性。在表中插入或更新项目时，GSI 不会同步更新。在正常操作条件下，向全局二级索引的写入操作将在几分之一秒内得到传播。在极少数故障情况下，时间可能会延长。正因如此，您的应用程序逻辑 应具备相应的能力，以处理可能过期的 GSI 查询结果。请注意，对于其他支持最终一致性读取的 DynamoDB API，它们也具有与此相同的行为。

比方说，有一个用于追踪最高分的表，该表中每个项目都具有 *UserId*、*GameTitle* 和 *TopScore* 属性。主分区键是 *UserId*，主排序键是 *GameTitle*。如果应用程序为 *GameTitle*“TicTacToe”和 *UserId*“GAMER123”添加了一个新的最高分的项目，随后再查询 GSI，则这个新分数可能不在查询结果之列。不过，一旦完成 GSI 传播，该新项目即开始出现在对 GSI 的此类查询中。

### 问：在全局二级索引扫描中，结果是怎么排列的？

对于全局二级索引，当采用仅分区键架构时，不会发生排序问题。对于具有分区-排序键架构的全局二级索引，同一分区键检索结果的排序是根据排序属性决定的。

### 问：什么是本地二级索引？

通过本地二级索引可以进行一些常规的查询操作，从而实现运行速度加快且运行成本最优，否则，其将需要检索大量项目，然后再对结果进行筛选。这表示您的应用程序可以基于更广泛属性进行更灵活的查询。

启动本地二级索引前，如果您想在某个分区查找特定项目（共享同一分区键的项目），DynamoDB 将提取共享单一分区键的所有对象，然后对结果进行相应筛选。以某种电子商务应用程序为例，它将用户订单数据存储在 DynamoDB 表中，该表采用客户 ID-订单时间戳这种分区-排序架构。在没有 LSI 的情况下，如果要“显示客户 X 提交的发货日期在最近 30 天内的所有订单，按发货日期予以排序”，您必须使用 Query API 来检索分区键“X”下的所有对象，按照发货日期对结果进行排序，然后过滤掉较早的记录。

借助本地二级索引，我们就可以简化上述操作了。现在，您可以在“发货日期”属性上创建索引，并有效执行此查询，仅需检索必需项 即可。由于您只需检索符合您所需特定标准的项目，因此大大减少了等待时间和查询成本。此外，由于您无需再写入自定义逻辑来筛选结果，因此，这一操作还简化 了应用程序的编程模型。我们将这种新二级索引称为“本地”二级索引，由于它与分区键结合使用，因此您可以在分区键存储桶内进行本地搜索。这样一来，即使以 前您或许只能借助分区键和排序键进行搜索，但现在，您还可以使用二级索引代替排序键进行搜索，从而增加了能够用于有效查询的属性数量。

可以将数据属性的冗余备份复制到您定义的本地二级索引中。这些属性包括表分区和排序键，以及您定义的备用排序键。您还可以将其他数据属性重复存储在本地二级索引中，从而在无需访问表本身的情况下，即可实现访问这些其他属性。

本地二级索引并非适用于所有应用程序。它们会对您可以在单一分区键数值中存储的数据量有一些限制。如需更多信息，请参阅下面有关项目集合的常见问题。

### 问：什么是投影？

被复制到本地二级索引中的属性集称为“投影”。投影将确定您能够以最高效方式进行检索的属性。查询本地二级索引 时，Amazon DynamoDB 可以访问任意具有相同性能特点的投影属性，此操作与访问其自身表中的属性方式相同。如果您需要检索尚未投影的任意属性，那么 Amazon DynamoDB 会自动从表中将这些属性提取出来。

定义本地二级索引后，您需要指定投影到索引的属性。每个索引条目至少应包括：(1) 表分区键值，(2) 用作索引排序键的属性，以及 (3) 表排序键值。

除此之外，您还可以选择用户指定其他非键属性，将其投影到索引。您还可以选择将所有属性投影到索引，在这种情况下，索引将复制与表相同的数据，但此数据按照您指定的备用排序键进行组织。

### 问：如何创建 LSI？

您需要在表创建时创建 LSI。随后将无法添加。如需创建 LSI，请指定以下两项参数：

索引排序键 – 将被索引和查询的属性。

投影属性 – 表中的属性列表，可直接将其复制到本地二级索引中，因此这些属性返回速度更快，且无需从包含表的所有项的主索引中提取数据。没有投影属性的情况下，本地二级索引仅含主索引和二级索引键。

### 问：如何创建本地二级索引？

必须在创建表时定义本地二级索引。表的主索引必须使用分区-排序复合键。

### 问：如何扫描本地二级索引？

如需扫描本地二级索引，除您想要查询的表名称外，还须明确引用索引。您必须指定索引分区属性名称和值。您可以针对索引键排序属性选择性地指定条件。

您的扫描可检索主索引中存储的非投影属性，其方式为执行表提取操作，且其需要占用附加读取容量单位。

### 问：本地二级索引扫描是否允许我在要返回的结果集中指定非投影属性？

本地二级索引扫描将支持抓取非投影属性。

### 问：主键的选择会如何影响我所能实现的可扩展性？

存 储数据时，Amazon DynamoDB 会将表分为多个分区，并根据主键的分区键元素来分布数据。分配容量资源时，Amazon DynamoDB 在所有主键上采取一种相对随机的访问模式。您应该建立您的数据模型，以使您的请求产生的流量在各个主键之间分布非常均匀。如果表的少数几个分区键元素的访 问量非常大，或者有单个分区键元素的使用量非常大，则流量将集中在少数几个分区上，甚至可能只集中在一个分区上。如果工作负载严重不平衡（即不成比例地集 中在一个或几个分区上），则操作将无法达到的预置的总体吞吐量级别。为了充分利用 Amazon DynamoDB 吞吐量，应让表中的分区键元素具有大量不同的值，而且对这些值的请求应该非常均匀，越随机越好。例如，如果应用程序有很多客户，并且对各个客户记录所做的 请求比较均匀，则 CustomerID 就是适合的主键。而“Product Category Name”就是一个严重不均衡的主键，因为其中的某些产品类别比其余类别更受欢迎。

### 问：什么是读取/写入容量单位？

如 何估计应用程序所需的读取和写入容量单位数量？一个写入容量单位能支持您每秒对最大 1KB 的项目执行一次写入操作。同样，一个读取容量单位让您能够每秒对最大 4KB 的项目执行一次强一致性读取（或执行两次最终一致性读取）。更大的项目将需要更多容量。您可以通过以下方式计算需要的读取和写入容量单位数量，估算每秒需 要执行的读取或写入次数，乘以项目的大小（进位到最接近的 KB）。

写入所需要的容量单位 = 每秒的项目写入量 x 1KB 块的项目大小

读取所需要的容量单位\* = 每秒的项目读取量 x 4KB 块的项目大小

\* 从每秒读取次数角度来看，如果您使用最终一致性读取，您会得到双倍的吞吐量。

如果项目的大小低于 1 KB，则每个读取容量单位将为您提供每秒一次的强一致性读取容量，每个写入容量单位将为您提供每秒一次写入的容量。例如，如果项目大小为 512 字节，您需要每秒从表中读取 100 个项目，则您需要预配置 100 个读取容量单位。

如 果项目的大小高于 4 KB，则您应该计算所需的读取容量和写入容量的单位数量。例如，如果项目大小为 4.5KB，您希望每秒进行 100 次强一致性读取，则需要预配置 100（每秒读取次数）x 2（存储 4.5KB 所需的 4KB 块量）= 200 个读取容量单位。

请 注意，需要的读取容量单位数量取决于每秒读取的项目数量，而不是 API 调用的数量。例如，如果您需要每秒从表中读取 500 个项目，而且这些项目大小为 4KB 或更小，则需要 500 个读取容量单位。无论您是进行 500 次单独 GetItem 调用，还是进行 50 次 BatchGetItem 调用并每次返回 10 个项目，都不会产生影响。

### 问：我始终都能达到配置吞吐量级别吗？

Amazon DynamoDB 在所有主键上采取一种相对随机的访问模式。您应该建立您的数据模型，以使您的请求产生的流量在各个主键之间分布非常均匀。如果访问模式非常不均匀或严重倾斜，则您将无法达到配置吞吐量级别。

存 储数据时，Amazon DynamoDB 会将表分为多个分区，并根据主键的分区键元素来分布数据。与表关联的配置吞吐量也在多个分区之间划分，每个分区的吞吐量基于所分配的配额进行单独管理。配 置吞吐量不在各个分区之间共享。因此，如果工作负载在分区键值之间分布得非常均匀，Amazon DynamoDB 中的表就能够最好地达到预置的吞吐量级别。在分区键值之间分布请求可将请求分布到各个分区，从而帮助您达到完整的预置吞吐量级别。

如果工作负载模式在主键之间分布不均匀，无法达到您的配置吞吐量级别，则您可以通过进一步提高配置吞吐量级别，为每个分区提供更高吞吐量，以满足吞吐量需求。但是，我们建议您考虑修改请求模式或数据模型，以实现主键之间的相对随机的访问模式。

### 问：副本表格的索引是否与主表格相同？

答：如果您选择通过复制应用程序创建副本表格，则主表格上的二级索引不会自动创建在副本表格上。复制应用程序不会将主表格的二级索引变化传播到副本表格中。您必须通过 AWS 管理控制台添加/更新/删除各个副本表格上的索引，就像处理常规 DynamoDB 表格一样。

### 问：副本表格的一致性模型是什么？

答：副本为异步更新。DynamoDB 会将主表格接受的写入操作确认为成功的写入操作。然后，写入操作会传播到各个副本。也就是说，写入操作传播到所有副本表格中之前会略有延迟。

### 问：DynamoDB 触发器的工作原理是什么？

答：DynamoDB 触发器的自定义逻辑以代码形式存储在 AWS Lambda 函数中。要为给定表格创建触发器，您可以关联 AWS Lambda 函数和 DynamoDB 表格上的流（通过 DynamoDB 流）。当表格更新时，更新便会发布到 DynamoDB 流中。相应地，AWS Lambda 会从关联的流中读取更新，并执行函数中的代码。

### 问：如果我删除了一个项目，此更改是否会反映在 DynamoDB 流中？

答：是的。DynamoDB 流中的每个更新都包含一个参数，用于指定更新是删除项目、插入新项目还是修改现有项目。

## VPC

### 问：Amazon VPC 有哪些组成部分？

Amazon VPC 由多个不同的数据元组成，它们对拥有现有网络的客户而言并不陌生：

* **Virtual Private Cloud (VPC)**：AWS 云中逻辑隔离的虚拟网络。从所选的范围内定义 VPC 的 IP 地址空间。
* **子网**：VPC 的 IP 地址范围内的一个区段，其中可放入各组隔离的资源。
* **Internet 网关**：公有 Internet 连接中的 Amazon VPC 这一端。
* **NAT 网关：一项高度可用的托管网络地址转换 (NAT) 服务，可便于私有子网中的资源访问 Internet。**
* **硬件 VPN 连接**：一种在您的 Amazon VPC 与数据中心、家庭网络或托管位置设施之间的基于硬件的 VPN 连接。
* **虚拟专用网关**：VPN 连接中的 Amazon VPC 这一端。
* **客户网关**：VPN 连接中的您这一端。
* **路由器**：路由器用于将子网互连，并在 Internet 网关、虚拟专用网关、NAT 网关和子网之间传输流量。
* **对等连接**：对等连接可以通过两个对等 VPC 之间的私有 IP 地址来路由流量。
* **S3 的 VPC 终端节点**：使您可以在不使用 Internet 网关或 NAT 的情况下从 VPC 内访问 Amazon S3，以及使用 VPC 终端节点策略控制访问。

没有公有 IP 地址的实例可以通过 NAT 网关或 NAT 实例来传输流量，从而访问 Internet

### 问：可否在 VPC 中的 Amazon EC2 实例运行和/或停止时，更改其私有 IP 地址？

在实例或接口的生命周期内，主要私有 IP 地址将一直保留。次要私有 IP 地址则可随时分配、取消分配，或者在接口或实例之间移动。

EIP 地址只应该在被配置为将流量直接路由到 Internet 网关的子网中的实例上使用。EIP 无法用于配置为使用 NAT 网关或 NAT 实例访问 Internet 的子网中的实例。

实例与同一 VPC 中其他子网内的 Amazon EC2 实例通信。利用 VPC 路由器，子网、Internet 网关和虚拟专用网关也可以互相通信。

除了安全组外，通过网络访问控制列表 (ACL) 也可允许或拒绝进出各个子网的网络流量

VPC 中的安全组指定允许传入或传出 Amazon EC2 实例的流量。网络 ACL 则在子网级别上运作，评估进出某个子网的流量

网络 ACL 执行无状态筛选，而安全组则执行有状态筛选。

### 问：有状态筛选和无状态筛选有什么区别？

有状态筛选可跟踪请求的来源，并可自动允许将请求的回复返回到来源计算机。例如，允许入站流量进入 Web 服务器上的 TCP 端口 80 的有状态筛选器将允许返回流量（通常为编号较高的端口，如目标 TCP 端口 63）通过客户端与 Web 服务器之间的有状态筛选器。筛选设备维护一个状态表，跟踪来源和目标端口编号与 IP 地址。筛选设备上仅需要一条规则：允许流量进入 Web 服务器的 TCP 端口 80。

无状态筛选则相反，仅检查来源或目标 IP 地址和目标端口，而忽略流量是新请求还是对请求的回复。上例中的筛选设备上需要实施两条规则：一条规则用于允许流量在 TCP 端口 80 上进入 Web 服务器，另一条规则用于允许流量传出 Web 服务器（TCP 端口范围 49、152 到 65、535）。

VPC 中使用由 Amazon EBS 支持的 AMI 启动的实例将在停止和重新启动后保持相同的 IP 地址。这与相似的实例从 VPC 之外启动时相反，那时会获取新的 IP 地址。子网中任何停止的实例的 IP 地址将视为不可用。

### 问：是否需要 Internet 网关才能使用对等连接？

否。VPC 对等连接不需要 Internet 网关。

### 问：没有公有 IP 地址的实例如何访问 Internet？

没有公有 IP 地址的实例可以通过以下两种方式之一访问 Internet：

1. 没有公有 IP 地址的实例可以通过 NAT 网关或 NAT 实例来传输流量，从而访问 Internet。这些实例使用 NAT 网关或 NAT 实例的公有 IP 地址来访问 Internet。NAT 网关或 NAT 实例允许出站通信，但不允许 Internet 上的计算机主动连接具有私有地址的实例。
2. 对于通过硬件 VPN 或 Direct Connect 进行连接的 VPC，实例可以将其 Internet 流量通过虚拟专用网关下传到现有的数据中心。它可从该处借助现有出口点和网络安全/监控设备访问 Internet。

### 问：可否在 VPC 中的 Amazon EC2 实例运行和/或停止时，更改其私有 IP 地址？

1. 在实例或接口的生命周期内，主要私有 IP 地址将一直保留。次要私有 IP 地址则可随时分配、取消分配，或者在接口或实例之间移动。

### 问：可否将一个或多个弹性 IP (EIP) 地址分配给基于 VPC 的 Amazon EC2 实例？

可以。不过，这些 EIP 地址只能从 Internet 访问（不能通过 VPN 连接访问）。每个 EIP 地址必须与实例上的一个唯一私有 IP 地址关联。EIP 地址只应该在被配置为将流量直接路由到 Internet 网关的子网中的实例上使用。EIP 无法用于配置为使用 NAT 网关或 NAT 实例访问 Internet 的子网中的实例。

### 问：Amazon VPC 路由器可以做什么？

Amazon VPC 路由器可以让子网中的 Amazon EC2 实例与同一 VPC 中其他子网内的 Amazon EC2 实例通信。利用 VPC 路由器，子网、Internet 网关和虚拟专用网关也可以互相通信。无法从路由器获得网络使用统计数据，但可使用 Amazon CloudWatch 从实例获取网络使用统计信息。

### 问：如何确保在 VPC 中运行的 Amazon EC2 实例的安全？

Amazon EC2 安全组可用来帮助确保 Amazon VPC 内实例的安全。VPC 中的安全组可用于指定允许进出各个 Amazon EC2 实例的进站和出站网络流量。没有显式允许进出实例的流量将自动被拒绝。

除了安全组外，通过网络访问控制列表 (ACL) 也可允许或拒绝进出各个子网的网络流量。

### 问：VPC 中的安全组和 VPC 中的网络 ACL 有什么区别？

VPC 中的安全组指定允许传入或传出 Amazon EC2 实例的流量。网络 ACL 则在子网级别上运作，评估进出某个子网的流量。网络 ACL 可通过设置允许和拒绝规则来进行使用。Network ACL 不能筛选同一子网中实例之间的流量。此外，网络 ACL 执行无状态筛选，而安全组则执行有状态筛选。

### 问：有状态筛选和无状态筛选有什么区别？

有状态筛选可跟踪请求的来源，并可自动允许将请求的回复返回到来源计算机。例如，允许入站流量进入 Web 服务器上的 TCP 端口 80 的有状态筛选器将允许返回流量（通常为编号较高的端口，如目标 TCP 端口 63）通过客户端与 Web 服务器之间的有状态筛选器。筛选设备维护一个状态表，跟踪来源和目标端口编号与 IP 地址。筛选设备上仅需要一条规则：允许流量进入 Web 服务器的 TCP 端口 80。

无状态筛选则相反，仅检查来源或目标 IP 地址和目标端口，而忽略流量是新请求还是对请求的回复。上例中的筛选设备上需要实施两条规则：一条规则用于允许流量在 TCP 端口 80 上进入 Web 服务器，另一条规则用于允许流量传出 Web 服务器（TCP 端口范围 49、152 到 65、535）。

### 问：可否从 Amazon VPC 中的 Amazon EBS 卷启动 Amazon EC2 实例？

可以。不过，VPC 中使用由 Amazon EBS 支持的 AMI 启动的实例将在停止和重新启动后保持相同的 IP 地址。这与相似的实例从 VPC 之外启动时相反，那时会获取新的 IP 地址。子网中任何停止的实例的 IP 地址将视为不可用。

### 问：是否需要 Internet 网关才能使用对等连接？

否。VPC 对等连接不需要 Internet 网关。

Cloudformation

### 问：AWS CloudFormation 与 AWS Elastic Beanstalk 有什么区别？

这些服务的设计目的是使二者相辅相成。[AWS Elastic Beanstalk](https://aws.amazon.com/elasticbeanstalk/) 提供了一个可在云中轻松部署和运行应用程序的环境。它与开发人员工具相集成，为您管理应用程序生命周期提供了“一站式”体验。AWS CloudFormation 是一种便捷的预配置机制，适用于众多 [AWS 资源](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-supported-resources.html)。它支持许多不同类型的应用程序的基础设施需求，如现有的企业级应用程序、旧式应用程序、使用各种 AWS 资源构建的应用程序，以及基于容器的解决方案（包括使用 AWS Elastic Beanstalk 构建而成的解决方案）。

AWS CloudFormation 支持 Elastic Beanstalk 应用程序环境，将其作为其中一种 AWS 资源类型。例如，这可使您创建和管理 AWS Elastic Beanstalk 托管的应用程序，以及用于存储应用程序数据的 RDS 数据库。除了 RDS 实例，还可向该组添加任何其他受支持的 AWS 资源。

### 问：我为什么不能命名全部资源？

尽管 AWS CloudFormation 允许您命名一些资源（如 Amazon S3 存储桶），但它并不允许您命名全部资源。命名资源限制了模板的可重复使用性，并会在资源因更新而需被替换时导致命名冲突。为了最大限度地减少这些问题的发 生，CloudFormation 会根据每个案例的具体情况决定是否支持资源命名。

CloudFront

### 问：什么是 Amazon CloudFront？

Amazon CloudFront 是一种 Web 服务，为企业和 Web 应用程序开发人员提供一种简单且经济高效的内容分配方法，不仅延迟低，而且数据传输速度高。与其他 AWS 服务相同，Amazon CloudFront 也是一种按用量付费的自助服务，无需长期承诺或最低费用。使用 CloudFront，您的文件将通过一个全球节点网络来传输至最终用户。

### 问：如何使用 Amazon CloudFront？

要使用 Amazon CloudFront，您必须执行以下操作：

* 对于静态文件，请将最终版本的文件存储在一个或多个原始服务器上。它们可以是 Amazon S3 存储段。对于动态生成的个性化或自定义内容，您可以使用 Amazon EC2 或其他任何 Web 服务器作为原始服务器。这些原始服务器将存储或生成要通过 Amazon CloudFront 分配的内容。
* 通过简单的 API 调用在 Amazon CloudFront 上注册您的原始服务器。此调用将返回一个 CloudFront.net 域名，您可以使用该域名，通过 Amazon CloudFront 服务从您的原始服务器分配内容。例如，您可以注册 Amazon S3 存储段“bucketname.s3.amazonaws.com”作为所有静态内容的来源，注册一个 Amazon EC2 实例“dynamic.myoriginserver.com”作为所有动态内容的来源。然后，您可以使用 API 或 AWS 管理控制台来创建 Amazon CloudFront 分配，它可能返回“abc123.cloudfront.net”作为分配域名。
* 将 cloudfront.net 域名或您创建的别名记录别名包括在您的 Web 应用程序、媒体播放器或网站中。使用 cloudfront.net 域名（或您设置的别名记录）发出的每个请求都被路由到最适合以最高性能分配内容的节点。该节点将尝试使用文件的本地副本来处理请求。如果本地副本不可 用，Amazon CloudFront 将从来源获取副本。然后，此副本将能够在该节点使用，以便处理今后的请求。

### 问：Amazon CloudFront 与 Amazon S3 有何不同？

* Amazon CloudFront 是分配经常访问的静态内容的理想之选，可从节点传输中受益 – 例如常用的网站图像、视频、多媒体文件或软件下载。

### 问：我可以选择仅处理来自价格较低的 Amazon CloudFront 地区的内容吗？

是的，“价格分级”让您能够选择以较低的价格将内容传输到 Amazon CloudFront 以外的地方。默认情况下，Amazon CloudFront 会通过其全球节点网络传输内容，以便尽量降低终端用户的延迟性。但是，因为在成本高的地区我们的收费也更高，这意味着在某些地区您需要支付更多费用才能以 较低的延迟性传输您的内容。价格分级能让您将 Amazon CloudFront 的高价节点排除在 Amazon CloudFront 服务分配范围之外，从而节省传输费用。此类情况下，Amazon CloudFront 将从属于您所选价格级别的地区内的节点传输您的内容，并根据传输内容的实际地区的数据传输和请求定价进行收费。

如果您最关注性能，则无需进行任何操作；您的内容将通过我们的整个节点网络传输。但是，如果您希望使用其他价格级别，可以通过 AWS 管理控制台或 Amazon CloudFront API 配置您的分配。如果您选择了没有包括所有地区的价格级别，则某些查看者（特别是所在位置不属于您所选价格级别的查看者）遇到的延迟性可能高于从所有 Amazon CloudFront 节点传输内容的延迟性。

请注意，Amazon CloudFront 偶尔还会从没有包括在您所选价格级别中的地区的节点处理您的内容请求。发生此类情况时，我们只按照您所选价格级别中最低费率的地区向您收费。

### 问：Amazon CloudFront 是否缓存 POST 响应？

Amazon CloudFront 不会缓存对 POST、PUT、DELETE 和 PATCH 请求的响应，因为这些请求会通过代理返回原始服务器。您可以缓存对 OPTIONS 请求的响应。

### 问：Amazon CloudFront 是否支持付费内容或私有内容的访问控制？

是，Amazon CloudFront 具有一项针对私有内容的可选访问控制功能。启用此选项时，Amazon CloudFront 将对您的请求进行安全签名，仅在您允许时才传输文件。阅读 [CloudFront 开发人员指南](http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html)，了解此功能的详细信息。

CloudTrail

问：CloudTrail 有哪些优势呢？  
  
CloudTrail 能够记录在您的账户上进行的 API 调用，方便您查看用户的活动。CloudTrail 记录了关于每个 API 调用的重要信息，包括 API 名称、调用者的身份、API 调用发生的时间、请求参数以及 AWS 服务返回的响应元素。

问：我可以在一个 AWS 区域中创建多少个跟踪？  
  
在一个 AWS 区域中，您最多可以创建五个跟踪。应用到所有区域的跟踪会出现在每个区域中，并算作每个区域的一个跟踪。

问：我可以在一个 AWS 区域中创建多少个跟踪？  
  
在一个 AWS 区域中，您最多可以创建五个跟踪。应用到所有区域的跟踪会出现在每个区域中，并算作每个区域的一个跟踪。

问：CloudTrail 传送一个 API 调用事件需要多长时间？  
一般情况下，CloudTrail 会在 API 调用后 15 分钟内传送事件。

问：CloudTrail 每隔多久会向我的 Amazon S3 存储段传送日志文件？  
  
CloudTrail 大约每隔 5 分钟会向您的 S3 存储段传送日志文件。如果您的账户上没有进行 API 调用，则 CloudTrail 不会传送日志文件。

### 问：对于 AWS 账户，可以查找多长时间里的 API 活动？

您可以查找最近 7 天 AWS 账户中捕捉的 API 活动

### 问：什么是 CloudTrail 与 CloudWatch Logs 的集成？

CloudTrail 与 CloudWatch Logs 相集成可将 CloudTrail 捕获到的 API 活动传送给您指定的 CloudWatch Logs 日志组中的 CloudWatch Logs 日志流。

### 问：使用 KMS 的服务器端加密加密 CloudTrail 日志文件有哪些好处？

使用 [SSE-KMS](http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html) 进行 CloudTrail 日志文件加密可通过 KMS 密钥加密日志文件，从而为交付到 Amazon S3 存储桶的 CloudTrail 日志文件添加一个额外的安全层。默认情况下，CloudTrail 会使用 Amazon S3 服务器端加密加密交付到 Amazon S3 存储桶的日志文件。

### 问：我有一个接收并处理 CloudTrail 日志文件的应用程序。我需要对该应用程序进行任何更改吗？

借助 SSE-KMS，Amazon S3 会自动加密日志文件，因此，您无需对自己的应用程序做出任何更改。与往常一样，您需要确保应用程序拥有相应的权限，即：Amazon S3 GetObject 和 KMS Decrypt 权限。

## CloudWatch

问：是否可以访问已终止的 Amazon EC2 实例或已删除的 Elastic Load Balancer 的指标数据？  
是。Amazon CloudWatch 为已终止的 Amazon EC2 实例或已删除的 Elastic Load Balancer 存储 2 周的指标数据。

### 问：我可以对日志和 Amazon CloudWatch 执行哪些操作？

CloudWatch Logs 能够监控并存储日志，以帮助您更好地了解并运行系统和应用程序。当使用 CloudWatch Logs 处理日志时，它会使用现有的日志数据进行监控，因此您将无需修改代码。以下是您可以对 Amazon CloudWatch 和日志执行操作的两个示例：

实时监控应用程序和系统：您可以使用 CloudWatch Logs 通过日志数据近乎实时地监控应用程序和系统。例如，CloudWatch Logs 能够追踪应用程序日志中的出错次数，并在错误率超过指定阈值时向您发送通知。Amazon CloudWatch 使用日志数据进行监控，因此您将无需修改代码。

**长期保留日志：**您可以根据需要使用 CloudWatch Logs 在高持久性低成本存储中长期保存日志数据，无需担心耗尽硬盘空间。CloudWatch Logs Agent 能够支持您轻松快速地将已旋转和未旋转的日志文件从主机移动到日志服务系统。然后，您可以按需访问原始日志事件数据。

### 问：CloudWatch Logs Agent 以何种频率发送数据？

CloudWatch Logs Agent 在默认状态下每五秒发送一次日志数据，可由用户配置。

### 问：我可以查看多长时间的警报历史记录？

警报历史记录有效期为 14 天。要查看警报历史记录，请在 AWS 管理控制台登录 CloudWatch，选择左侧菜单中的“Alarms”，然后单击下方面板中的“History”选项卡。您可以在这里查找警报状态更改的历史记录以及警报配置修改。

### 问：我可以按固定的计划进行操作吗？

通过使用常见的 Unix cron 语法，CloudWatch Events 能够按您设定的计划生成事件。通过监控这些事件，您可实施计划应用程序。

### 问：CloudWatch Events 与 AWS CloudTrail 有什么区别？

CloudWatch Events 是一个近乎实时的系统事件流，用于描述 AWS 资源的更改。借助 CloudWatch Events，您可以定义规则，从而以自动方式监控特定的事件并执行相应操作。AWS CloudTrail 是一种服务，用于记录 AWS 账户的 API 调用并将包含 API 调用的日志文件发送到 Amazon S3 存储桶或 CloudWatch Logs 日志组。借助 AWS CloudTrail，您可以查看与 AWS 资源的创建、删除和修改有关的 API 活动历史记录，很可以排查运行和安全问题。

### 问：CloudWatch Events 与 AWS Config 有什么区别？

AWS Config 是一项完全托管型服务，可为您提供 AWS 资源库存、配置历史记录和配置更改通知，以增强安全性和方便管理。Config 规则可帮助您确定配置更改是否合规。CloudWatch Events 用于近乎实时地应对资源状态更改。它不会裁定这些更改是否符合政策，也不会像 Config/Config 规则那样提供详细的历史记录。它是一个通用的事件流。

## EBS

### 问：Amazon EC2 实例终止时，会对我的数据产生什么影响？

与保存在本地实例存储的数据（只要实例存在，数据就始终存在）不同，保存在 Amazon EBS 卷中的数据的存续不受实例寿命的影响。因此，我们建议您将本地实例存储仅用于临时数据，而对于需要保存较长时间的数据，我们建议您使用 Amazon EBS 卷，或将数据备份到 Amazon S3。如果将 Amazon EBS 卷用作根分区，而您希望在实例生命周期外保留 Amazon EBS 卷，请将“Delete On Terminate”标志设置为“No”。

### 问：我应该选择哪种卷？

Amazon EBS 提供两种主要存储类别：适用于交易型工作负载的 SSD 型存储（性能主要取决于 IOPS），以及适用于吞吐量密集型工作负载的 HDD 型存储（性能主要取决于吞吐量，以 MB/s 为单位）。SSD 型卷专用于交易型和 IOPS 密集型数据库工作负载、启动卷以及需要高 IOPS 的工作负载。SSD 型卷包括预配置 IOPS SSD (io1) 和通用型 SSD (gp2)。HDD 型卷专用于吞吐量密集型和大数据工作负载、大型 I/O 以及连续 I/O 模式。HDD 型卷包括吞吐量优化型 HDD (st1) 和 Cold HDD (sc1)。

### 问：应用程序读写的 I/O 大小是否会影响我从预配置 IOPS SSD (io1) 卷获得 IOPS 的速率？

会。对于给定的资源分配而言，您获得的 IOPS 速率取决您的应用程序读取和写入操作的 I/O 大小。**预配置 IOPS 卷以 256 KB 或以下的 I/O 大小处理您的应用程序读写。**I/O 大小每增加超过 256 KB 都会线性提升达到相同的 IOPS 速率所需的资源。例如，如果您配置了 500 IOPS 的卷，这意味着它每秒可以处理 500 个 256 KB 写入操作、250 个 512 KB 写入操作，或者 125 个 1024 KB 写入操作，以此类推。您可以使用 [Amazon CloudWatch](https://aws.amazon.com/cn/cloudwatch/) 监控您的吞吐量和 I/O 大小。

### 问：哪些因素会影响预配置 IOPS SSD (io1) 卷的性能一致性？

挂载到 EBS 优化型实例的预配置 IOPS SSD (io1) 卷可以提供一致性能，能在指定年度 99.9% 的时间内实现 10% 以内的预配置 IOPS 性能。有几个因素可能影响您看到的一致性水平。例如，拍摄快照会在快照待处理期间影响您从卷获得的 IOPS 速率。对于新创建的卷，您的 IOPS 速率可能也会较低。为了让新卷获得最大的性能一致性，我们建议您先在卷上读取或写入所有数据块，然后再投入服务。

另一影响性能的因素是您的应用程序是否没有发送足够的 I/O 请求。这可以通过查看卷的队列深度来监控。队列深度是您的应用程序向卷发起的待处理 I/O 请求的数量。为获得最大的一致性，在一分钟内，对于每 500 个预配置的 IOPS，预配置 IOPS 卷队列长度平均值（四舍五入取整数）必须保持为 1。例如，对于预配置了 1500 个 IOPS 的卷，队列长度平均值必须为 3。有关确保稳定的卷性能的更多信息，请参阅 [Increasing EBS Performance](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html)

### 问：应用程序读写的 I/O 大小是否会影响我从 HDD 型卷获得吞吐量的速率？

会。您获得的吞吐量速率取决于应用程序读写的 I/O 大小。**HDD 型卷以 1MB 的 I/O 大小处理读取和写入操作。**连续 I/O 会被合并和处理成 1MB 单元，每个非连续 I/O 也会被处理成 1MB，即使实际 I/O 小于 1MB。因此，虽然拥有小型随机 I/O 的交易型工作负载（如数据库）在 HDD 型卷上无法正常运行，但是连续 I/O 和大型 I/O 也会在较长时间后实现 st1 和 sc1 的预期性能。

### 问：我能否将多个卷一起条带化以获得更好性能？

能。您可以将挂载到较大 EC2 实例的多个卷一起条带化，以达到 48000 IOPS 或 800MB/s。不过，st1 和 sc1 的性能与卷大小呈线性扩展关系，因此将这些卷一起条带化可能没有多大益处。

### 问：对 16TB 的卷拍摄完整快照会不会比对 1TB 的卷更花时间？

不会，EBS 卷采用特殊设计，不管是对 16 TB 的卷还是 1 TB 的卷拍摄快照，时间都是一样的。

### 问：当预配置 IOPS 卷从实例断开连接时，是否会就预配置的 IOPS 给我计费？

会，当预配置 IOPS 卷从实例断开连接时，您就会因预配置 IOPS 被计费。当卷断开连接时，我们建议您创建一个快照并删除该卷以减少费用。更多相关信息，请参阅 [Trusted Advisor](http://aws.amazon.com/support/trustedadvisor/) 中的“Underutilized Amazon EBS Volumes”成本优化检查。  该项目检查您的 Amazon Elastic Block Store (Amazon EBS) 卷配置并在卷出现使用不足时发出警告。

## Elastic Beanstalk

问：使用 AWS Elastic Beanstalk，开发人员现在可以实现哪些以前无法实现的事情？  
AWS Elastic Beanstalk 可自动执行容量预配置、负载均衡、Auto Scaling 和应用程序部署的细节，创建一种运行某版应用程序的环境。您只需上传自己可部署的代码（如 WAR 文件）或推出 Git 存储库，剩余工作则可由 AWS Elastic Beanstalk 执行。借助 AWS Toolkit for Visual Studio 和 AWS Toolkit for Eclipse，即可将应用程序部署到 AWS Elastic Beanstalk 并进行管理，而不必离开 IDE。一旦应用程序运行，Elastic Beanstalk 将自动执行监控、应用程序版本部署、基本运行状况检查和促进日志文件访问等管理任务。使用 Elastic Beanstalk，开发人员可集中开发应用程序，无须再处理预配置服务器、设置负载均衡或管理扩展等面向部署的任务。

问：应用程序能多快进行扩展？  
AWS Elastic Beanstalk 使用 Auto Scaling 提供真正的弹性环境。您的应用程序可以配置为自动根据 CPU 使用率或网络带宽等阈值扩展数十或数百倍。使用 Elastic Beanstalk 控制台可以轻松为您特定的应用程序配置这些阈值。使用 Elastic Beanstalk，则无需担心是否能够快速扩展来处理高峰流量或用户，也不必担心是否会被迫为不需要的资源付费。

问：是否可以同时运行多个应用程序版本？可以。AWS Elastic Beanstalk 可用于支持多个运行环境，例如，一个用于集成测试，一个用于前期生产，一个用于生产。每个环境可独立配置并在其独自的 AWS 资源中运行。此外，Elastic Beanstalk 还能随时间推移存储和跟踪应用程序版本，以便可以轻松将现有环境回滚到早期版本，或使用早期版本启动新环境来尝试和再现客户问题。

问：是否可以使用 AWS Elastic Beanstalk 来部署必须具有高可用性的应用程序？可以。为此，您需要编辑环境配置设置，为“Auto Scaling”最小值选择 2 或以上个实例，并将多可用性区域设置为“Any 2”。设置 AWS 可用区域是为了外观上比较明确，故障独立，性能可靠。

### 问：AWS Elastic Beanstalk 是否在 Amazon S3 中存储任何内容？

是。AWS Elastic Beanstalk 会在 Amazon S3 中存储您的应用程序文件及服务器日志文件（可选）。如果使用 AWS 管理控制台、AWS Toolkit for Visual Studio 或 AWS Toolkit for Eclipse，系统会在您的账户中创建一个 Amazon S3 存储桶，并自动将您上传的文件从本地客户端复制到 Amazon S3。您还可以选择将 Elastic Beanstalk 配置为每小时复制服务器日志文件到 Amazon S3。通过编辑环境配置设置，可完成上述操作。

### 问：托管平台更新适用于何种平台版本更新？

Elastic Beanstalk 可以为新修补程序和次要平台版本自动执行平台更新。Elastic Beanstalk 不会自动执行主要平台版本更新（例如 Java 7 Tomcat 7 到 Java 8 Tomcat 8），因为这些更新包含向后不兼容的更改，且需要进行额外测试。在这些情况下，您必须手动启动更新。

### 问：在进行托管更新期间，我能对环境执行哪些操作？

在进行托管更新期间，您只能执行“中止”这一项操作。执行此操作后，系统将立即停止更新并回退到上一版本。

### 问：AWS Elastic Beanstalk 的费用是多少？

对于 AWS Elastic Beanstalk，您只需为存储和运行应用程序实际使用的 AWS 资源付费，没有额外费用。符合 AWS 免费套餐使用条件的新 AWS 客户可以使用 Elastic Beanstalk 的默认设置来部署免费套餐中运行的应用程序。

## ElasticCache

### 问：什么是 Amazon ElastiCache？

Amazon ElastiCache 是一种 Web 服务，让用户能够在[云](https://aws.amazon.com/cn/what-is-cloud-computing/)中 轻松部署和运行 Memcached 或 Redis 协议兼容服务器节点。Amazon ElastiCache 允许您从快速的托管型内存缓存系统检索信息，而不是完全依赖速度较慢的基于磁盘型数据库，从而提高 Web 应用程序的性能。本服务可简化和免除内存缓存环境的管理、监控和操作，让您的工程资源专注于应用程序开发。借助 Amazon ElastiCache，您不仅能够改善用户操作和查询的负载与响应时间，也可降低与扩展 Web 应用程序相关的成本。

Amazon ElastiCache 可自动化分布式缓存环境运行所需的常见管理任务。借助 Amazon ElastiCache，只需通过在 AWS 管理控制台内点击几下，几分钟内就能为您的应用程序架构添加缓存层面。预配置了缓存集群后，Amazon ElastiCache 可以自动检测和更换故障缓存节点，提供一个灵活的系统，减缓可降低网站和应用程序加载速度的数据库过载风险。通过与 Amazon CloudWatch 监控功能集成，Amazon ElastiCache 可以加强缓存节点相关的关键性能指标的可见性。Amazon ElastiCache 兼容 Memcached 和 Redis 协议，因此您在现有 Memcached 或 Redis 环境内使用的代码、应用程序和常用工具都能与本服务无缝协作。与所有 Amazon Web Services 相同，您无需预先投资，而且只需为所使用的资源付费。

问：什么是维护窗口？**我的缓存节点在软件维护期间是否可用？**

您可以将 Amazon ElastiCache 维护窗口视为在请求或需要的情况下执行软件修补的机会。如果在给定的星期内安排了“维护”事件，将在您确定的 60 分钟维护窗口的某个时间点启动和完成维护。

如果安排了软件修补，您的缓存节点将在维护窗口内出现短暂停机。有关详细信息，请参阅缓存引擎版本管理。软件修补可以是用户请 求的（如缓存软件升级），或者是按需确定的（如果我们发现系统或缓存软件中存在任何安全漏洞）。软件修补很少发生（通常几个月一次），并且几乎不需要过长 的维护时间。如果创建缓存节点时未指定首选周维护窗口，将分配默认值 60 分钟。如果希望在代表您执行维护时进行修改，您可以通过 AWS 管理控制台或使用 ModifyCacheCluster API 修改数据库实例来执行该操作。如果这样选择，您的各个缓存节点可以执行不同的首选维护窗口。

### 问：Amazon ElastiCache 的使用如何收费和记账？

按实际用量付费，而且没有最低费用。定价依据为每种节点所消耗的缓存节点小时数。未满一小时的按一小时计费。同一可用区域内的 Amazon EC2 和 Amazon ElastiCache 之间传输数据是免费的。不过，同一地区不同可用区域内的 Amazon EC2 实例和 Amazon ElastiCache 节点传输数据时，需支付标准的 Amazon EC2 地区数据传输费，您只需支付 Amazon EC2 实例的数据传入或传出费用。Amazon ElastiCache 节点本身传入或传出的流量并不需要支付 Amazon ElastiCache 数据传输费。有关更多信息，请参阅相关的[定价页面](https://aws.amazon.com/cn/elasticache/pricing/)。

### 问：如何控制对 Amazon ElastiCache 的访问？

不使用 [VPC](http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html) 时，Amazon ElastiCache 允许您通过缓存安全组来控制对缓存集群的访问。缓存安全组与防火墙的功能类似，控制对您的缓存集群的网络访问。默认情况下，您的缓存集群的网络访问处于关 闭状态。如果希望应用程序可以访问您的缓存集群，必须明确允许来自于特定 [EC2 安全组](http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html)中主机的访问。这个过程称为进入。

要允许通过网络访问您的缓存集群，需要创建缓存安全组，并将所需的 EC2 安全组（因此也须指定要允许的 EC2 实例）与其链接。您可以在创建时将安全组与缓存集群关联，或者使用 [AWS 管理控制台](https://console.aws.amazon.com/elasticache/)中的“Modify”选项。

请注意，目前缓存集群尚未启用基于 IP 范围的访问控制。缓存集群的所有客户端必须处于 EC2 网络中，并按照上文所述通过安全组授权。

使用 VPC 时，请参阅[此处](https://aws.amazon.com/cn/elasticache/faqs/#What_is_VPC_Why_Amazon_ElastiCache)了解更多信息。

### 问：我自己的数据中心服务器中运行的程序是否可以访问 Amazon ElastiCache？

不可以。目前，ElastiCache 集群的所有客户端必须处于 Amazon EC2 网络中，并按照[此处](https://aws.amazon.com/cn/elasticache/faqs/#How_do_I_control_access)所述通过安全组授权。

问：什么是 Amazon Virtual Private Cloud (VPC)？**为什么我可能需要用到 Amazon ElastiCache？**

Amazon VPC 允许您在 Amazon Web Services (AWS) 云中私有、隔离的部分创建虚拟网络环境，从中可以对专用 IP 地址范围、子网、路由表和网络网关等方面进行全面控制。借助 Amazon VPC，您可以定义虚拟网络拓扑和自定义网络配置，使其非常类似于您在自己的数据中心所操作的传统 IP 网络。

在以下情况下，您可能需要在 VPC 中使用 Amazon ElastiCache：您希望运行面向公众的 Web 应用程序，同时仍在私有子网中保留公众不可访问的后端服务器。您可以为 Web 服务器创建一个能访问 Internet 的公有子网，并将后端基础设施放在不能访问 Internet 的私有子网中。您的后端基础设施可以包含 RDS 数据库实例和一个提供了缓存层的 Amazon ElastiCache 缓存集群

### 问：在 VPC 内与在 VPC 外使用 Amazon ElastiCache 有何差别？

无论是否使用 VPC，Amazon ElastiCache 的基本功能都保持不变。无论您的 ElastiCache 缓存集群部署在 VPC 的内部还是外部，Amazon ElastiCache 均可管理自动故障检测、恢复、扩展、自动发现以及软件修补等任务。

类似地，无论 Amazon ElastiCache 缓存集群是在 VPC 的内部还是外部，都不可能从 Internet 进行访问。在 VPC 内，ElastiCache 缓存集群的节点只有一个专用 IP 地址（在您定义的子网内）。在 VPC 外，可使用缓存安全组来控制对 ElastiCache 缓存集群的访问，详情请参阅此处。

### 问：是否可以将 VPC 外部的现有 ElastiCache 缓存集群迁移到 VPC 内部？

不可以，您不能将 VPC 外的现有 Amazon ElastiCache 缓存集群迁移到 VPC 内。您需要在 VPC 内创建一个新的 Amazon ElastiCache 缓存集群。

### 问：是否可以使用缓存安全组来配置 VPC 内的缓存集群？

不可以，因为在 VPC 内运行时，不使用缓存安全组。相反地，它们在非 VPC 环境下使用。在 VPC 内创建缓存集群时，您将需要使用 VPC 安全组。

### 问：基于 Memcached 的 Amazon ElastiCache 可以用来缓存什么内容？

您可以使用本服务缓存多种数据元，如永久数据存储中的内容（如 Amazon RDS、SimpleDB 或 EC2 上驻留的自管理型数据库等）、动态生成的网页（如使用 Nginx 生成），或者可能不需要永久存储支持的瞬变会话数据。也可以用它来实施高频计数器，以便在高容量 Web 应用程序中部署允入控制。

### 问：如何为我的应用程序选择适当的缓存节点类型？

虽然此问题没有准确的答案，但使用 Amazon ElastiCache 时，您无需担心是否获得恰当数量的缓存节点，因为以后您都能随时轻松添加或删除节点。在选择初始配置时，您可以考虑以下两个互为关联的因素：

* 达到目标缓存命中率所需的缓存总内存量，以及
* 保持可接受的应用程序性能且不会在缓存节点故障时造成数据库过载所需的缓存节点数。

所需的内存量取决于您的数据集的大小，以及应用程序的访问模式。要提高容错能力，在对所需的内存总量有初步概念之后，可将该内 存量分割为足够数量的缓存节点，以便您的应用程序在一两个缓存节点出现故障时依然可以运行。例如，如果您的内存要求为 14GB，则可能需要使用两个 cache.m1.large 节点，而不是一个 cache.m1.xlarge 节点。需要确保一个或多个缓存节点故障恢复期间缓存命中率出现临时降低时，数据库等其他系统不会过载，这一点很重要。

问：什么是自动发现？**它对我有什么帮助？**

Auto Discovery 是帮助开发人员节省时间和精力，并降低应用程序复杂性的一种功能。向 Amazon ElastiCache 缓存集群添加或删除缓存节点时，Auto Discovery 可以通过客户端实现缓存节点的自动发现。到目前为止，为了应对集群成员资格的变动，开发人员仍须手动更新缓存节点的终端节点列表。根据客户端应用程序的构 建方式，一般而言，需要进行客户端初始化，其方法是关闭和重启应用程序，而这会导致停机。但通过 Auto Discovery，我们可以摆脱这种复杂性。利用 Auto Discovery，除了可向后兼容 Memcached 协议以外，Amazon ElastiCache 还向客户端提供有关缓存集群成员资格的信息。能够处理更多信息的客户端，无需任何初始化操作便能自我再新配置，从而使用 Amazon ElastiCache 缓存集群的最新节点。

### 问：如果继续用我自己的 Memcached 客户端搭配使用 ElastiCache 缓存集群，是否可以享受此功能？

不可以，使用现有的 Memcached 客户端将不能享受 Auto Discovery 功能。要使用 Auto Discovery 功能，客户端必须能够使用配置终端节点并确定该集群节点的终端节点。您可以使用 Amazon ElastiCache 集群客户端

### 问：什么是基于 Redis 的 Amazon ElastiCache？

基于 Redis 的 Amazon ElastiCache 是一种 Web 服务，让用户能够在云中轻松部署和运行 Redis 协议兼容的服务器节点。该项服务可进行 Redis 节点的管理、监控和运行；而节点的创建、删除和修改可通过 ElastiCache 控制台、命令行接口或 Web 服务 API 执行。基于 Redis 的 Amazon ElastiCache 支持 Redis 主/从复制。

### 问：基于 Redis 的 Amazon ElastiCache 为节点故障提供了哪些选项？

基于 Redis 的 Amazon ElastiCache 将通过请求新的服务资源修复节点，而后将节点的现有 DNS 名称重定向到新的服务资源。因此，Redis 节点的 DNS 名称将保持不变，但 Redis 节点的 IP 地址可能会不时改变。如果您拥有的复制组具有一个或多个只读副本，并且已经启用了多可用区，那么在主节点发生故障时，ElastiCache 将自动检测故障，选择副本并将其提升为新的主节点。它还将传播 DNS，从而使您可以继续使用主终端节点，并在提升后指向新提升的主节点。有关更多详细信息，请参阅此常见问题的“[Multi-AZ](https://aws.amazon.com/cn/elasticache/faqs/#redis-multi-az)” 部分。在禁用多可用区的情况下选择 Redis 复制选项时，如果主节点发生故障，您可以选择启动故障转移到只读副本节点。故障转移目标可以在同一个区域或另一个区域中。为了使故障恢复到原区域，将原区 域中的只读副本提升为主节点。您可以选择架构您的应用程序，从而使 Redis 客户端库重新连接到已修复的 Redis 服务器节点。由于有些 Redis 库会在遇到通信错误或超时时无限期停止使用服务器，所有这一点很有用。

### 问：主节点故障期间，我的只读副本是否可用？

可以，主节点故障期间，只读副本可继续服务请求。主节点以修复的节点或提升后的只读副本形式恢复后，只读副本短时间内将不能服务任何请求，因为它们要同步主节点中的缓存信息。

### 问：基于 Redis 的 Amazon ElastiCache 是否支持 Redis 的密码功能？

否，基于 Redis 的 Amazon ElastiCache 不支持 Redis 密码。这是因为配置文件中所存储的密码的固有局限性。基于 Redis 的 Amazon ElastiCache 之集群与 EC2 安全组相关，而非依靠 Redis 密码，并且只有此安全组中的客户端才有权访问 Redis 服务器。

### 问：能否降级至较低的引擎版本？

不能。不支持降级至较低的引擎版本。

### 问：能否缩减至较小的节点类型？

目前不支持迁移至较小的节点类型。

### 问：如何为给定的主缓存节点部署只读副本节点？

使用 CreateReplicationGroup API 或在 Amazon ElastiCache 管理控制台中单击几下鼠标即可很快创建一个只读副本。创建复制组时，您要指定 MasterCacheClusterIdentifier。MasterCacheClusterIdentifier 是您想从中进行复制的“主”缓存集群的缓存集群标识符。然后，您可以通过调用 CreateCacheCluster API 指定主要集群的 ReplicationGroupIdentifier 和 CacheClusterIdentifier，以在复制组中创建只读副本集群。跟标准的缓存集群一样，您也可以指定可用区域。启动创建只读副本 时，Amazon ElastiCache 将对主缓存集群拍摄快照，并开始复制。因此，在拍摄快照时，您的主缓存集群上的 I/O 可能会短暂性停止。I/O 停止一般大约会持续一分钟。

删除只读副本同创建一样简单；只需使用 Amazon ElastiCache 管理控制台或调用 DeleteCacheCluster API 即可（为您要删除的只读副本指定 CacheClusterIdentifier）。

### 问：我可以为给定的主缓存节点创建多少个只读副本？

此时，Amazon ElastiCache 允许您为给定的主缓存节点最多创建五 (5) 个只读副本。

### 问：如果发生故障转移，只读副本会怎么样？

如果发生故障转移，所有关联和可用的只读副本在故障转移完成后将自动恢复复制（获取最新提升的只读副本的更新）。

### 问：是否可以将我的只读副本提升为“独立的”主缓存节点？

不可以，不支持此操作。但是，您可以为您的基于 Redis 的 ElastiCache 节点拍摄快照（可以选择主节点或任何只读副本）。然后，您可使用快照“播种”新的基于 Redis 的 ElastiCache 主节点。

### 问：只读副本是否会与其主缓存节点一起保持最新状态？

主缓存节点的更新会自动复制到所有关联的只读副本。不过，鉴于 Redis 的异步复制技术，出于各种原因，只读副本更新可能会落后于其主缓存节点。常见的原因包括：

* 主缓存节点的 I/O 写入量超过了将更改应用于只读副本的速率。
* 主缓存节点和只读副本之间有网络分区或延迟

只读副本受 Redis 复制的优点和缺点影响。如果使用只读副本，您应了解只读副本与其主缓存节点之间可能存在滞后或“不一致”。单击此处了解如何找出只读副本“不一致”的指南。

### 问：我的只读副本已远远落后于主缓存节点。我应该怎么办？

如前述问题中所述，使用 Redis 异步复制时，只读副本与其主缓存节点之间的“不一致”或滞后非常常见。如果现有只读副本已远远落后而不能满足您的要求，您可以重启该副本。副本滞后可能会随时间推移自然而然地加大和缩小，具体取决于您的主缓存节点的稳定状态使用模式。

问：只读副本的成本是多少？**如何计算记账周期？**

只读副本按标准的缓存节点进行计费，且费率相同。和标准的缓存节点一样，只读副本的每“缓存节点小时”费率取决于只读副本的缓 存节点类 – 有关最新的定价信息，请参阅 Amazon ElastiCache 详细信息页面。在主缓存节点和只读副本之间复制数据，产生的数据传输不收取费用。只读副本的账单周期从成功创建只读副本后开始（即当列出的状态为“有效” 时）。只读副本将一直按标准的 Amazon ElastiCache 缓存节点小时费用计费，直到您发布命令将其删除为止。

问：执行故障转移时会发生什么状况？**这种情况会持续多长时间？**

Amazon ElastiCache 支持启动故障转移，这样您可以尽快恢复缓存操作。故障转移后，Amazon ElastiCache 会轻松翻转缓存节点的 DNS 记录指向只读副本，只读副本转而成为新的主节点。我们鼓励您遵循最佳做法，在应用程序层实施缓存节点连接重试。通常，故障转移从开始到结束会在三到六分钟 内完成。

### 问：是否可以在另一个地区创建只读副本作为我的主节点？

不可以。您只可以在相同地区的同一可用区域或不同可用区域预配置您的只读副本作为您的主缓存节点

### 问：Redis 的 ElastiCache 复制组的多可用区是什么？

Redis 的 ElastiCache 复制组由一个主节点和多达五个只读副本组成。Redis 将数据从主节点中异步复制到只读副本中。在特定类型的计划维护期间或不太可能发生的 ElastiCache 节点故障或可用区故障期间，Amazon ElastiCache 将自动探测主节点的故障、选择一个只读副本并将其提升为新的主节点。ElastiCache 还将传送所提升只读副本的 DNS 更改，因此，如果您的应用程序正在写入主节点的终端节点，则不需要更改终端节点。

### 问：当主节点发生故障时，将提升哪个只读副本？

如果只读副本不止一个，将提升向主节点进行异步复制时延迟最小的只读副本。

### 问：“备份与恢复”如何发挥作用？

一旦启动备份，ElastiCache 将拍摄特定 Redis 集群的快照，之后可将其用于恢复或存档。您随时可以选择启动备份，也可以设置一个保留期长达 35 天每天重复进行的备份。

当您选择一个快照进行恢复时，将会创建一个新的基于 Redis 的 ElastiCache 集群并填充快照中的数据。您可以通过这种方式从一个特定的快照创建多个基于 Redis 的 ElastiCache 集群。

ElastiCache 目前使用 Redis 的原生机制创建 RDB 文件并将其存储为快照。

### 问：我的快照存储在哪里？

快照存储在 S3 中。

### 问：基于 Memcached 的 ElastiCache 是否支持“备份与恢复”？

否，快照仅适用于基于 Redis 的 ElastiCache。

### 问：拍摄快照对性能有什么影响？

拍摄快照时，节点延迟可能会在短时间内增加。快照使用 Redis 内置的 BGSAVE，因此受其优点和缺点的影响。尤其是当 Redis 进程分叉时，父进程将继续为请求提供服务，而子进程将数据存储在磁盘上然后退出。快照生成期间，分叉会增加内存使用率。当此内存使用率超过缓存节点可用内 存的使用率时，将会触发交换，进一步降低节点速度。鉴于此，我们建议对一个只读副本生成快照（而非主集群）。此外，我们建议设置预留内存参数，以将交换使 用率降至最低。请参阅[此处](http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/Snapshots.html)查看更多详情。

### 问：我可以从基于 Redis 的 ElastiCache 只读副本创建快照吗？

可以。从只读副本创建快照是备份数据同时将性能影响降至最低的最佳方式。

### 问：我可以将快照从一个区域复制到其他区域吗？

可以。您必须首先将快照复制到在同一区域内选择的授权 S3 存储桶中，然后使用 S3 PUT object – Copy API 将其复制到其他区域内的存储桶。

Classic 负载均衡器适用于在多个 EC2 实例之间进行简单的负载均衡，而应用程序负载均衡器则适用于需要向多个服务路由流量的微服务或基于容器的架构，或适用于在同一 EC2 实例的多个端口之间进行负载均衡的情况。

### 问：Classic 负载均衡器与应用程序负载均衡器在功能上有哪些异同？

下表展示了这两种负载均衡器的关键功能。

|  |  |  |
| --- | --- | --- |
| **功能** | **Classic 负载均衡器** | **应用程序负载均衡器** |
| 支持的协议 | HTTP、HTTPS、TCP、SSL | HTTP、HTTPS、HTTP/2、WebSocket |
| 支持的平台 | EC2-Classic、EC2-VPC | EC2-VPC |
| 粘性会话 (Cookie) | 是 | 是 |
| 后端服务器身份验证 | 是 | 否 |
| 空闲连接超时 | 是 | 是 |
| 连接排空 | 是 | 是 |
| 跨区负载均衡\* | 是 | 始终启用 |
| 运行状况检查 | 是 | 已增强 |
| CloudWatch 指标 | 是 | 已增强 |
| 访问日志 | 是 | 已增强 |
| 基于路径的路由 | 否 | 是 |
| 动态端口 | 否 | 是 |
| 删除保护 | 否 | 是 |

\* 对于应用程序负载均衡器，跨区负载均衡始终处于启用状态；对于 Classic 负载均衡器，该选项默认处于禁用状态，但可以根据需要启用或禁用。

问：Classic 负载均衡器是否支持 IPv6 流量？  
支持。每个 Classic 负载均衡器都关联一个 IPv4、一个 IPv6 和一个双栈（同时支持 IPv4 和 IPv6）DNS 名称。目前 VPC 中不支持 IPv6。

## EMR

### 问：Amazon EMR 有什么作用？

Amazon EMR 能即时灵活配置自身所需容量大小，执行数据密集型应用计算，完成诸如 Web 索引、数据挖掘、日志文件分析、机器学习、财务分析、科学模拟和生物信息研究等任务。Amazon EMR 技术让您专注于数据分析，无需担心费时的 Hadoop 集群设置、管理或调整，也无需担心所需要的计算能力。

Amazon EMR 可有效解决需要快速、高效处理大量数据之类的问题。借助 Web 服务界面，您可以构建处理工作流程并以编程方式监控集群的运行进度。此外，您还可以使用 AWS 管理控制台简洁的 Web 界面启动集群，并监控对 Amazon EC2 实例集群进行的处理密集型计算。

### 问：使用 Amazon EMR 可以做到哪些之前我无法做到的事情？

对于耗时的设置和管理工作，Amazon EMR 可大幅降低其复杂性。和优化数据所在的 Hadoop 集群或计算容量的复杂程度。您在几分钟内即可立即开始加速处理大型 Hadoop 集群，无需等待数小时或数天。 除非您另有指定，否则集群在完成处理后将自动终止，因此您无需为不再需要的资源付费。

使用此服务，可以快速执行应用程序的数据密集型任务，例如，Web 检索、数据挖掘、日志文件分析、机器学习、财务分析、科学模拟及生物信息研究。

作为软件开发人员，您也可以运行自己更为复杂的应用程序，允许您添加计划、工作流、监控等其他特性与功能。

### 问：EMR 最佳做法有哪些？

如果您在生产中运行 EMR，那么应该指定 AMI 版本、Hive 版本、Pig 版本等等， 以确保版本不会出现意外更改（例如，当 EMR 稍后添加对于较新版本的支持时就会如此）。 如果您的集群属于关键任务型，那么请仅在任务节点上使用竞价型实例，因为竞价型实例价格上涨时您会失去这些实例。 在开发中，请使用记录并启用调试以便更快地找出和纠正错误。 如果您使用的是 GZIP，请将文件大小控制在 1 – 2GB 之间，因为 GZIP 文件无法拆分。 单击[此处](https://aws.amazon.com/whitepapers/emr-best-practices/)下载有关 Amazon EMR 最佳实践的白皮书。

### 问：如何启动集群？

您可以通过在 AWS 管理控制台中填写简单的集群请求表启动集群。 在请求表中，需要指定集群的名称、Amazon S3 中输入数据的位置、处理应用程序、理想的数据输出位置、希望使用的 Amazon EC2 实例数量和类型。 您也可以指定一个存储集群日志文件和 SSH 密钥的位置，以便在集群运行时进行登录。 此外，您可以使用 RunJobFlow API 或在命令行工具中使用 ‘create’ 命令启动集群

### 问：是否可向已在运行的集群添加步骤？

是。一旦任务运行后，您可以通过 AddJobFlowSteps API 选择性地添加更多步骤。AddJobFlowSteps API 将向当前的步骤序列结尾添加新的步骤。您可能希望使用此 API 在集群中执行条件逻辑或进行调试。

### 问：Amazon EMR 支持哪些操作系统版本？

当前，Amazon EMR 支持 32 位和 64 位模式的 Debian/Squeeze。

### 问：为什么必须注册 Amazon SimpleDB 才能使用集群调试？

Amazon EMR 将在您的 Amazon SimpleDB 账户下存储 Hadoop 作业、任务和任务尝试的状态信息。您可以[在此](https://aws.amazon.com/cn/simpledb/)订阅 Amazon SimpleDB。

### 问：Amazon EMR 是否支持 Amazon EC2 按需实例、竞价型实例和预留实例？

是。Amazon EMR 可无缝支持按需实例、竞价型实例和预留实例。[单击此处](http://aws.amazon.com/ec2/faqs/#What_is_a_Reserved_Instance)详细了解 Amazon EC2 预留实例。[单击此处](http://aws.amazon.com/ec2/spot/)详细了解 Amazon EC2 竞价型实例。

### 问：在集群执行过程中，如何防止其他用户查看我的数据？

Amazon EMR 在两个 Amazon EC2 安全组中启动您的实例，一组用于主实例，另一组用于从实例。主安全组的端口是开放的，以便与服务进行通信。它的 SSH 端口也呈开放状态，以允许您使用启动时指定的密钥 SSH 到实例。从实例在单独的安全组中启动，仅允许与主实例进行交互。默认情况下，两个安全组都设置为不允许从属于其他客户的 Amazon EC2 实例等外部源进行访问。由于这些是您账户内的安全组，所以您可以使用标准 EC2 工具或控制面板重新配置它们。[单击此处](http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html)详细了解 EC2 安全组。

### 问：我的数据的安全性如何？

Amazon S3 提供身份验证机制，确保存储的数据安全以防被未授权访问。除非上传数据的客户另行指定，否则仅该用户才能访问数据。Amazon EMR 客户还可以选择使用确保安全传送的 HTTPS 协议将数据发送到 Amazon S3。此外，Amazon EMR 始终使用 HTTPS 在 Amazon S3 与 Amazon EC2 之间发送数据。为提高安全性，客户可以在将输入数据上传到 Amazon S3 前对其加密（使用任何常见的数据压缩工具）；然后，当 Amazon EMR 从 Amazon S3 提取数据时，则需要在其集群的开头添加解密步骤。

### 问：我应选择哪个地区来运行集群？

创建集群时，通常应选择您的数据所在的区域。

### 问：Amazon EMR 如何使用 Amazon EC2 和 Amazon S3？

客户将其输入数据和数据处理应用程序上传到 Amazon S3。然后，Amazon EMR 按客户指定启动一定数量的 Amazon EC2 实例。该服务开始执行集群，同时使用 S3N 协议将输入数据从 Amazon S3 推入启动的 Amazon EC2 实例。一旦集群完成后，Amazon EMR 即可将输出数据传输到 Amazon S3，客户在此可以取回数据或将其用作其他集群的输入数据。

### 问：在 Amazon EMR 中如何进行计算？

Amazon EMR 使用 Hadoop 数据处理引擎来执行 MapReduce 编程模型中实施的计算。客户可根据 map() 和 reduce() 函数执行其算法。该服务可启动客户指定数量的 Amazon EC2 实例，其中包含一个主实例和多个从实例。Amazon EMR 在这些实例上运行 Hadoop 软件。主节点将输入数据划分成数据块，并将数据块处理分配到从节点。然后，每个从节点对分配给它的数据运行 map 函数，生成中间数据。然后，对中间数据排序和分区，并将其发送到对之应用缩减器函数的进程。这些节点也可在从节点上运行。最后，在文件中收集缩减器任务的 输出。一个“集群”可能包含一系列上述 MapReduce 步骤。

### 问：如果集群中的主节点出现故障，Amazon EMR 是否可以使其恢复？

不会。如果主节点出现故障，集群将会终止，您必须返回任务。 Amazon EMR 当前不支持主节点自动故障转移或主节点状态恢复。如果主节点出现故障，AWS 管理控制台将显示“主节点被终止”消息，向您指示启动新的集群。 客户可以在其集群中实施检查点，以便在 Amazon S3 中保存中间数据（在集群尚未缩减时创建的数据）。 这样，在出现故障时将能够从最后一个检查点恢复集群。

### 问：如果集群中的从节点出现故障，Amazon EMR 是否可以从其恢复？

是。Amazon EMR 对于从节点故障具有容错功能，当从节点出现故障时将继续执行任务。在当前版本中，Amazon EMR 不会自动预配置其他节点来接管出现故障的从节点。

### 问：是否可以修改正在运行的集群中的从节点数？

是。从节点有两种类型：(1) 核心节点，既可使用 Hadoop 分布式文件系统 (HDFS) 托管持续性数据，又能运行 Hadoop 任务；以及 (2) 任务节点，仅用来运行 Hadoop 任务。当集群运行时，您可以增加核心节点的数量，也可以增加或减少任务节点的数量。 通过 API、Java 软件开发工具包或命令行客户端可以执行该操作。请参阅开发人员指南中的[调整运行的集群](http://docs.amazonwebservices.com/ElasticMapReduce/latest/DeveloperGuide/ResizeJobFlow.html)部分，了解如何修改运行的集群大小的详细信息。

### 问：我何时会希望使用核心节点与任务节点？

由于核心节点在 HDFS 中托管持续性数据而无法删除，所以应为核心节点预留所需的容量，直到集群完成。 由于任务节点可以添加或删除且不含 HDFS，所以它们非常适合仅临时需要容量的情况。

### 问：为什么我会希望修改正在运行的集群中的从节点数？

在某些情况下，您可能会希望修改正在运行的集群中的从节点数。 如果您的集群运行速度低于预期或时间要求发生变化，您可以增加核心节点数来提高集群性能。 如果集群的不同阶段有不同的容量需求，您可以开始使用少量核心节点，并随时增加或减少任务节点的数量来满足集群不断变化的容量要求。

### 问：是否可以在集群终止后保留 EBS 卷上的数据？

目前，Amazon EMR 将在集群终止后删除卷。如果您希望在集群生命周期外保留数据，不妨考虑将 Amazon S3 作为数据存储使用。

## Glacier

**之间进行取舍？**

Amazon S3 是耐用、安全、简单且快速的存储服务，是专为开发人员简化 Web 级计算而设计。如果您需要快速或频繁地访问数据，则建议采用 Amazon S3。如果存储成本是最先考虑的因素，很少取回数据，且可以接受取回数据时间为数小时，则建议采用 Amazon Glacier。

Amazon S3 现在提供了新的存储选项，让您能够利用成本极低的 Amazon Glacier 存储服务来为数据存档。您可以定义 S3 生命周期规则，以便自动将 Amazon S3 数据元存档到 Amazon Glacier，从而帮您降低存储成本。您可以访问 Amazon S3 Developer Guide 中的 [Object Lifecycle Management](http://docs.amazonwebservices.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html) 主题了解更多信息。

### 问：Amazon Glacier 的收费如何？

利用 Amazon Glacier，存储价格为每月每 GB 0.007 USD，您只需为所用的资源付费。因此，不存在安装费用，而对于大部分存档用例，总花费将主要由存储成本组成。

上传和取回请求的价格是每 1 000 个请求 0.05 USD。如果是[取回大量](https://aws.amazon.com/cn/glacier/faqs/#How_will_I_be_charged_when_retrieving_large_amounts_of_data_from_Amazon_Glacier)数据，则会收取取回费，起始价格为每 GB 0.01 USD。另外，对于未满 [90 天即被删除](https://aws.amazon.com/cn/glacier/faqs/#How_am_I_charged_for_deleting_data_that_is_less_than_3_months_old)的数据，需按比例支付费用，标准为每 GB 0.021 USD。由于 Amazon Glacier 是专用于存储经常访问且长久使用的数据，这些恢复收费和提早删除费对大部分人可能都不会发生。

当我们的成本较低时，我们的收费也比较低。有些价格因 Amazon Glacier 区域而不同，具体取决于您的文件库的位置。在同一区域内的 Amazon EC2 和 Amazon Glacier 之间传输数据，不收取数据传输费。对于在所有其他区域的 Amazon EC2 和 Amazon Glacier 之间传输的数据（例如，在 Amazon EC2 加利福尼亚北部区域和 Amazon Glacier 美国东部弗吉利亚北部区之间），将按照传输两端的互联网数据传输费率进行收费。

### 问：可以免费取回多少数据？

您每月最多可以免费取回存储在 Glacier 中数据的 5%。一般而言，这足以满足您备份和归档需要。每月 5% 的最高免费取回限额是按日比例计量的。例如，您在某一天，有 12 TB 的 数据存档在 Glacier 中，那么这一天您可以免费恢复 20.5 GB 的数据（假定该月为 30 天，则为：12 TB x 5% / 30 天 = 20.5 GB）。

### 问：删除存储不足 3 个月的数据时，如何收费？

Amazon Glacier 是专为需要长久保留数据的使用案例设计的。如果要删除的档案已存储达到 3 个月或以上，则从 Amazon Glacier 删除数据是免费的。如果档案在上传后 3 月内就要删除，则需要支付提早删除费用。在美国东部（弗吉利亚北部）区域，如果在三个月内删除，则按比例计算的提早删除费每 GB 0.021 USD。如果您上传数据 1 个月后，删除了 1GB，则提早删除费为 0.014 USD。然而，如果您 2 个月后删除了 1GB，则提早删除费为 0.007 USD。

### 问：我的数据是否已加密？

是的，本服务中的所有数据均将在服务器端进行加密。Amazon Glacier 可为您处理密钥管理和密钥保护事宜。Amazon Glacier 使用了一种强大的分组加密技术：256 位高级加密标准 (AES-256)。256 位是为 AES 定义的最大密钥大小。如果客户希望自己管理密钥，可在上传数据前将其加密。

### 问：如何从该服务检索数据？

您可以使用服务的 REST API 直接从该服务下载数据。当您请求从 Glacier 取回数据时，即表示您启动了一个取回作业。取回作业完成后，数据在 24 小时可供您下载。取回作业一般会在 3 到 5 小时内完成。

### 问：如果我设置了“最大检索速度”且我的检索超出了免费套餐范围，如何计算我的存储费用？

我们来假设您每天有 10 GB 的[免费检索允许量](https://aws.amazon.com/cn/glacier/faqs/#How_much_data_can_I_retrieve_for_free)且您设置了 20 GB/小时的“最大检索速度”，从而在 AWS 控制台中显示的数据检索估计费用为“144.00 USD/月或以下”（假设在美国东部区域，且一个月为 30 天）。

现在我们来逐步了解几个情景，假设这是个新的月份。

第 1 天，您发出了 8 GB 存档的检索请求。由于 8 GB 低于该日的免费检索允许量，您的检索请求将被接受，且数据检索免费。

第 2 天，您的同事不慎发出了 100 GB 存档的检索请求。由于检索速度（基于 4 小时的完成时间）为 100 GB/4 小时 = 25 GB/小时，超出了 20 GB/小时的“最大检索速度”，请求将被拒绝且不会产生数据检索费用。

第 3 天，您发出了一个 40 GB 存档的检索请求。由于所有的数据检索计费都假设检索在 4 小时内完成，40 GB/4 小时产生的检索速率为 10 GB/小时，这低于您设置的 20 GB/小时的“最大检索速度”，所以您的检索请求被接受。您该日的可计费最大检索速度为（40 GB – 10 GB 免费套餐）除以 4 小时，即 7.5 GB/小时。该月，您的估计数据检索帐单在此时为 7.5 GB/小时 \* 0.01 USD/GB\* 720 小时/月 = 54 USD，这低于控制台中所显示的数据检索估计费用 144.00 USD/月。

第 4 天，您在发出 40 GB 存档的检索请求后立即发出了 44 GB 存档的请求。40 GB 存档的请求被接受，因为检索速度（基于 4 小时的完成时间）为 40 GB/4 小时 = 10 GB/小时，这低于 20 GB/小时的“最大检索速度”。但检索 44 GB 存档的第二个请求遭到了拒绝，因为，尽管单就该请求而言，仅产生 44 GB/4 小时 = 11 GB/小时的检索速率，但第一个检索请求仍在进程中。如果第二个请求被接受，则合并后的最大检索速度将为 10 GB/小时 + 11 GB/小时 = 21 GB/小时，这超出了您指定的 20 GB/小时的最大检索速度。您决定等到第二天再检索 44 GB 的存档。

第 5 天，您收到消息，在客户的要求下，需要尽快提供 44 GB 存档以及另一个 36 GB 的存档。这意味着您需要同时检索两个存档，也就等于发出产生 20 GB/小时检索速率的 80 GB 检索请求，这正好等于您设置的“最大检索速度”。您发出了这两个请求，且它们都被接受。您的可计费最大检索速度为（80 GB – 10 GB 免费套餐）/ 4 小时 = 17.5 GB/小时，您的数据检索估计费用为 17.5 GB/小时 \* 0.01 USD/GB\* 720 小时/月 = 126.00 USD/月，根据 20 GB/小时的最大检索速度，这低于 AWS 控制台中显示的 144.00 USD/月。这一新的估计值超过了第 3 天的估计费用 54 USD/月。如果您在该月剩下的日子没有产生其他数据检索费用，则您该月的数据检索费用为 126.00 USD，低于控制台中显示的 144.00 USD/月的估计值。

### IAM

问：IAM 可以解决什么问题？  
IAM 可以让多个用户轻松安全地访问您的 AWS 资源。IAM 让您能够：

* 管理 IAM 用户及其访问权限：您可以通过 AWS 的身份管理系统创建用户，向用户发放个人安全证书（例如，访问密钥、密码、[多重验证](https://aws.amazon.com/cn/iam/details/mfa/)设备），或请求为其提供[临时安全证书](http://docs.aws.amazon.com/STS/latest/UsingSTS/Welcome.html)，以为用户提供 AWS 服务和资源的访问权限。您可以指定权限，限制用户可执行的操作。
* 管理[联合用户](https://aws.amazon.com/cn/iam/details/manage-federation/)的访问 – 您可以为您在公司目录中管理的用户请求包含可配置有效期限的安全证书，以便让您的员工和应用程序可以安全访问您 AWS 账户中的资源，而不必为其创建 IAM 用户账户。您可以为这些安全证书指定权限，控制用户可执行的操作。

问：哪些人可以管理 AWS 账户的用户？  
AWS 账户持有者可以管理用户、组、安全证书和权限。此外，您也可以向单个用户授予权限，以便他们能通过调用 IAM API 管理其他用户。例如，可以创建管理员用户为公司管理用户，这也是推荐的做法。用户获得您授予的管理其他用户的权限后

问：可否将多个 IAM 角色与一个 EC2 实例关联？  
否。目前一个 EC2 实例只能关联一个 IAM 角色

### 问：我能否将托管策略用作基于资源的策略？

托管策略只能挂载到 IAM 用户、组或角色。您不可以将其用作基于资源的策略。

### 问：我如何使用策略设置精细权限？

使用策略，您可以指定若干权限粒度层级。首先，您可以定义想要允许或明确拒绝访问的特定 AWS 服务操作。其次，根据具体操作，您可以定义可对其执行这些操作的特定 AWS 资源。第三，您可以定义指定策略何时生效的条件（例如，是否启用了 MFA）。

### 问：策略是什么样的？

以下策略授予访问权限以便在特定存储桶 example\_bucket 中的特定文件夹 example\_folder 中添加、更新和删除对象。

{  
   "Version":"2012-10-17",  
   "Statement":[  
      {  
         "Effect": "Allow",  
         "Action":[  
            "s3:PutObject",  
            "s3:GetObject",  
            "s3:GetObjectVersion",  
            "s3:DeleteObject",  
            "s3:DeleteObjectVersion"  
         ],  
         "Resource":"arn:aws:s3:::example\_bucket/example\_folder/\*"  
      }  
   ]  
}

问：IAM 用户如何登录？  
IAM 用户必须使用账户的登录 URL 登录，此 URL 将把他们定向到可以输入其 IAM 用户名和密码的页面。此登录 URL 位于 IAM 控制台的仪表板中。AWS 账户的系统管理员必须将该登录 URL 告知 IAM 用户。

问：临时安全证书有什么好处？  
临时安全证书有以下功能：

* 扩展您的内部用户目录以启用至 AWS 的联合，从而使您的员工和应用程序能够安全地访问 AWS 服务 API，而无需为其创建 AWS 身份。
* 为无限数量的联合用户申请临时安全证书。
* 配置临时安全证书的失效时间，当您通过移动设备访问 AWS 服务 API 有遗失设备的风险时提供更高安全保障。

问：是否能在到期前撤消临时安全证书？  
不能。请求临时证书时，我们推荐以下操作：

* 创建临时安全证书时，请将过期设置为适合您的应用程序的值。

由于无法限制根账户的权限，因此建议您在创建临时安全证书时使用 IAM 用户，不要使用根账户。您可以撤销 IAM 用户的发布源调用以请求该证书的权限。此操作几乎会立即撤消由该 IAM 用户颁发的所有临时安全证书的特权。

问：联合用户能否访问 AWS API？  
能。您可以通过编程方式为联合用户提出临时安全证书请求，使之能安全地直接访问 AWS API。我们提供了一份[示例应用程序](http://aws.amazon.com/code/1288653099190193)并展示了如何启用身份联合，让通过 Microsoft Active Directory 维护的用户可以访问 AWS 服务 API。有关更多信息，请参阅“[使用临时安全凭证以请求对 AWS 资源进行访问](http://docs.aws.amazon.com/STS/latest/UsingSTS/using-temp-creds.html)”。

问：如果我为 AWS 根账户或 IAM 用户启用了 AWS MFA，他们是否始终需要输入 MFA 代码才能直接调用 AWS API？  
不是，它是可选的。不过，如果您计划调用由 MFA 保护的 API 访问保证安全的 API，则必须输入 MFA 代码。

如果使用 AWS 根账户或 IAM 的访问密钥调用 AWS API，则无需输入 MFA 代码。出于安全方面的原因，我们建议您删除 AWS 根账户的所有访问密钥，而使用具有所需权限的 IAM 用户的访问密钥调用 AWS API。

问：MFA 保护的 API 访问如何与现有的 MFA 使用案例（例如 S3 MFA Delete）交互？  
MFA 保护的 API 访问与 S3 MFA Delete 彼此不进行交互。S3 MFA Delete 当前不支持临时安全证书。相反，要调用 S3 MFA Delete API，必须使用长期访问密钥。

问：MFA 保护的 API 访问是否适用于联合用户？  
客户无法使用 MFA 保护的 API 访问来控制联合用户的访问。GetFederatedSession API 不接受 MFA 参数。由于联合用户不能使用 AWS MFA 设备进行身份验证，因此他们无法访问使用 MFA 保护的 API 访问指定的资源。

### KMS

**为什么应该使用 AWS KMS？**

如果您是一个需要加密应用程序中的数据的开发人员，您应该将 AWS 软件开发工具包用于 AWS KMS 支持，以轻松使用和保护加密密钥。如果您是一个 IT 管理员，您想找到一个可扩展的密钥管理基础设施来支持您的开发人员以及越来越多的应用程序，您应该使用 AWS KMS 降低您的许可成本和运营负担。如果您负责证明数据安全性以实现法规或合规性之目的，您应该使用 AWS KMS 来验证数据在所使用和存储的应用程序间进行了一致加密。

**为什么使用信封加密？为什么不只是将数据发送到 AWS KMS 中直接加密？**

由于 AWS KMS 支持发送小于 4 KB 的数据进行加密，信封加密可提供巨大的性能优势。当您使用 KMS 直接加密数据时，数据必须通过网络传输。信封加密可为您的应用程序或 AWS 云服务降低网络负载。只有通过 KMS 对数据密钥的请求和履行必须通过网络。由于数据密钥始终以加密形式存储，因此在您需要它进行操作时可轻松安全地分配该密钥，而无需担心它会被泄露。加密的 数据密钥会发送到 AWS KMS 中并使用主密钥进行解密，从而最终允许您解密数据。数据密钥直接提供在应用程序中，您不必将整个数据块发送到 AWS KMS 中和忍受网络延迟。

**我可以导入什么类型的密钥？**

您可以导入 256 位对称密钥。

**我能否从 AWS KMS 中导出一个主密钥并将其用于我自己的应用程序中？**

不能。为帮助确保主密钥的安全，使您的策略能得到一致性实施并提供集中化的该密钥使用日志，只能在 AWS KMS 中创建和使用主密钥。

**AWS KMS 与 AWS CloudHSM 相比如何？**

AWS CloudHSM 为您提供一个安装在 Amazon Virtual Private Cloud (VPC) 中的专用硬件设备，从而提供一个 FIPS 140-2 2 级验证单租户 HSM 来存储和使用您的密钥。您对您的密钥和将密钥用于 CloudHSM 的应用程序软件有完全控制权。

AWS KMS 可使您控制您的应用程序和受支持 AWS 服务通过单个控制台在全世界多个区域使用的加密密钥。在 AWS KMS 中对您所有的密钥进行集中化管理可使您实施谁能使用您的密钥，它们何时轮换以及谁能管理它们的策略。AWS KMS 与 AWS CloudTrail 的集成使您能够审计您的密钥使用情况，以支持法规和合规性活动。

### Lambda

### 问：什么时候应该使用 AWS Lambda 与 Amazon EC2？

Amazon Web Services 提供一组计算服务以满足各种需求。

[Amazon EC2](https://aws.amazon.com/cn/ec2/) 具有范围广泛的实例类型以及自定义操作系统、网络和安全设置以及整个软件堆栈的选项，可提供灵活性，从而让您能够将现有的应用程序轻松迁移到云中。使用 Amazon EC2，您将负责预配置容量、监控服务器队的运行状况和性能，并设计容错性和可扩展性。[AWS Elastic Beanstalk](https://aws.amazon.com/cn/elasticbeanstalk/) 提供易用的服务，**供您部署和扩展 Web 应用程序，**您可以在其中保留对底层 EC2 实例的所有权和完整控制权。[Amazon EC2 Container Service](https://aws.amazon.com/cn/ecs/) 是一项可扩展的管理服务，支持 Docker 容器，允许您轻松地在 Amazon EC2 实例的托管集群上运行分布式应用程序。

**AWS Lambda 可用于依照对事件的响应轻松执行代码，如 Amazon S3 存储桶的更改、Amazon DynamoDB 表的更新或您的应用程序或设备生成的自定义事件。**利用 Lambda，您不必预配置您自己的实例；Lambda 会代您执行所有的运行和管理活动，包括容量预配置、监控服务器队运行状况、向底层计算资源应用安全补丁、部署您的代码、在前端运行 Web 服务以及监控和记录您的代码。AWS Lambda 为您的代码提供轻松的扩展和高可用性，从而无需您做额外努力。

### 问：AWS Lambda 函数为什么必须是无状态的？

保持函数的无状态性可使 AWS Lambda 按需要尽可能多地启动函数副本，从而扩展到传入事件的速率。由于 AWS Lambda 的编程模式是无状态的，因此您的代码可以通过调用其他 Web 服务，如 Amazon S3 或 Amazon DynamoDB，来访问有状态的数据。

### 问：哪些限制适用于 AWS Lambda 函数代码？

Lambda 试图尽量不对正常的语言和操作系统活动强加限制，但仍有些活动被禁用的：入站网络连接受 AWS Lambda 管理，只支持 TCP/IP 套接字，且黑盒（调试）系统调用受限制。TCP 端口 25 流量同样受到限制，以防垃圾信息。

### 问：如何监控 AWS Lambda 函数？

AWS Lambda 会代您自动监控 Lambda 函数，从而通过 Amazon CloudWatch 实时报告指标，包括请求总数、延迟、出错率和节流请求。通过 Amazon CloudWatch 控制台或 AWS Lambda 控制台，可以查看每一个 Lambda 函数的统计信息。您还可以在您的 Lambda 函数中调用第三方监控 API。请访问[故障排除 CloudWatch 指标](http://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions.html)了解更多信息。使用 Lambda 的内建指标会依照 AWS Lambda 的标准费率计费。

### 问：什么是事件源？

事件源是 AWS 服务或开发人员创建的应用程序，用于生成可触发 AWS Lambda 函数使其运行的事件。有些服务通过直接调用云函数（例如 Amazon S3）向 Lambda 发布这些事件。Lambda 也可以在未向 Lambda 发布事件的其他服务中轮询资源。例如，Lambda 可以从 Kinesis 数据流中拉取记录并为数据流中的每条消息执行 Lambda 函数。

通过登录到 Amazon S3 并使用 S3 存储桶通知，就可将 AWS CloudTrail 等其他很多服务简单地用作触发 AWS Lambda 函数的事件源。

**问题：AWS Lambda 如何处理来自 Amazon Kinesis 流和 Amazon DynamoDB 流的数据？**

发送到您的 AWS Lambda 功能的 Amazon Kinesis 和 DynamoDB 流记录将根据分片进行严格序列化。这意味着，如果您将两个记录放在同一个分片中，则 Lambda 保证将首先通过第一条记录来调用您的 Lambda 功能，然后再通过第二条记录来调用。如果第一条记录的调用超时，或者遇到任何其他错误，则 Lambda 将重试直至其成功（或者记录达到其 24 小时过期时间），然后才会对下一条记录采取操作。无法保证不同分片之间记录的排序，并且每个分片的处理是平行进行的。

### 问：AWS Lambda 函数的可用性如何？

AWS Lambda 旨在通过复制和冗余来向服务本身和其操作的 Lambda 函数提供高可用性。二者皆无维护窗口期或计划停机时间。

### 问：对于一次可以执行的 AWS Lambda 函数的数量有没有限制？

没有。AWS Lambda 采用的设计可以支持大量函数实例并列运行。但是，AWS Lambda 有一项默认的安全阈值：每区域每账户 100 个并发执行绪。如果您想申请提高 100 个并发执行绪或每秒调用数的默认限制，可以访问[支持中心](https://aws.amazon.com/support)，单击“Open a new case”，然后发出服务限制提升请求。

### 问：如果 Lambda 函数在处理事件时发生故障会怎样？

如遇故障，进行同步调用的 Lambda 函数会返回异常信息。异步调用的 Lambda 函数会重试至少 3 次，之后事件将被拒绝。Amazon Kinesis 流和 Amazon DynamoDB 流中的事件会反复重试，直到 Lambda 函数成功或数据过期。Kinesis 和 DynamoDB 流会将数据保留 24 小时。

问：一个 Lambda 函数是否可以访问多个 VPC？不可以。Lambda 函数只能访问一个 VPC。如果指定多个子网，则所有子网都必须位于同一个 VPC 中。您可以通过在 VPC 之间建立对等连接来连接到其他 VPC。

问：一个 VPC 中的 Lambda 函数是否还能够访问 Internet 和 AWS 服务端点？在默认配置下，配置为可访问特定 VPC 中资源的 Lambda 函数将无法访问 Internet。如果您需要访问外部端点，则需要在 VPC 中创建 [NAT](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html)，以转发相应流量并将安全组配置为允许这些出站流量。

### RDS

问：什么是维护窗口？**我的数据库实例在软件维护期间是否可用？**

如有请求或要求，您可以通过 Amazon RDS 维护窗口控制数据库实例修改（例如，扩展数据库实例类别）及软件补丁更新时间。如果在给定一周内安排了维护工作，则在制定维护时段内的某个时间点启动和完成维护。维护时间为 30 分钟。

**唯一需要使用 Amazon RDS 将数据库实例脱机的情况是扩展计算操作（从始至终通常只需要几分钟时间）或要求修补软件的情况。只有安全和耐久的补丁会自动安排要求的修补。**这种修补很少 发生（通常几个月一次），并且几乎不会要求过长的维护窗口。如果创建数据库实例时未指定首选周维护窗口，将分配默认值 30 分钟。如果希望在代您执行维护时进行修改，您可以通过 [AWS 管理控制台](https://console.aws.amazon.com/)或使用 ModifyDBInstance API 修改数据库实例来执行该操作。如果这样选择，您的各个数据库实例可以执行不同的首选维护窗口。

采用[多可用区部署](https://aws.amazon.com/cn/rds/faqs/#36)的方式运行数据库实例可进一步降低维护事件的影响。有关详细信息，请参阅 [Amazon RDS 用户指南](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html)。

有关使用 API 或命令行界面指定维护窗口的更多信息，请参阅 [Amazon RDS 开发人员指南](http://docs.amazonwebservices.com/AmazonRDS/latest/DeveloperGuide/)。有关多可用区域模式部署的更多信息，请[单击此处。](https://aws.amazon.com/cn/rds/faqs/#36)

### 问：如果我的查询运行缓慢，应该怎么办？

如果使用的是 MySQL，您可以访问数据库的 MySQL 慢查询日志来确定是否存在运行缓慢的 SQL 查询以及各个查询（如有）的性能特征。您可以设置“slow\_query\_log”数据库参数并查询 mysql.slow\_日志表，以查看慢运行的 SQL 查询。有关详细信息，请参阅 [Amazon RDS 用户指南](http://docs.amazonwebservices.com/AmazonRDS/latest/UserGuide/Appendix.MySQL.CommonDBATasks.html)。

如果使用的是 Oracle，您可以使用 Oracle 跟踪文件数据来确定慢查询。有关访问跟踪文件数据的更多信息，请参阅 [Amazon RDS 用户指南](http://docs.amazonwebservices.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.CommonDBATasks.html#Appendix.Oracle.CommonDBATasks.WorkingWithTracefiles)。

如果使用的是 SQL Server，您可以使用客户端 SQL Server 跟踪文件来确定慢查询。有关访问服务器端跟踪文件数据的信息，请参阅 [Amazon RDS 用户指南](http://docs.amazonwebservices.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.CommonDBATasks.html#Appendix.SQLServer.CommonDBATasks.WorkingWithTracefiles)。

您还可以通过 [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/) 查看数据库实例的 CPU 使用率指标。高级别的 CPU 使用率会降低查询性能，因此您可能会考虑扩展数据库实例的等级。有关监控 CPU 使用率的更多信息，请阅读 [Amazon RDS 监控指南](http://developer.amazonwebservices.com/connect/entry.jspa?externalID=2934)。

### 问：Amazon RDS 的使用如何收费和计费？

仅按实际使用量收费，无最低费用或设置费用。您的计费依据为：

* 数据库实例小时数 – 基于使用的数据库实例的等级（例如，标准、小、大、超大型）。数据库实例运行未满一小时的按一小时计费。
* 存储（每月每 GB）– 您的数据库实例预配置的存储容量。如果您在计费期内扩展了预配置的存储容量，则将按相应比例计费。
* 每月的 I/O 请求 – 您的存储 I/O 请求总数量*（仅限于 Amazon RDS 磁性存储）*
* 每月的预配置 IOPS – 预配置 IOPS 数量，不论 IOPS 的消耗量如何*（仅限于 Amazon RDS 预配置 IOPS (SSD) 存储）*
* 备份存储 – 备份存储是指与自动数据库备份和拍摄的有效数据库快照相关联的存储。延长备份保留期或增加快照拍摄数量，将增加数据库所消耗的备份存储。Amazon RDS 免费提供与您预配置的数据库存储同等大小的备份存储。例如，如果您每月预配置的数据库存储为 10GB，我们将每月免费提供多达 10GB 的备份存储。根据我们作为数据库管理员的经验，备份绝大多数数据库需要的原始存储量要少于主数据集；这意味着大多数客户始终都不必为备份存储付费。仅有效 数据库实例的备份存储免费。
* 数据传输 – 传入和传出数据库实例的 Internet 数据传输。

### 问：如果对预留实例等级进行扩展或缩小，我的预留会发生什么状况？

每个预留都会关联下面一组属性：数据库引擎、数据库实例等级、部署类型、许可模式和区域。在持续期限内，每个预留只能用于属性相同的数据库实例。如果您要 在预留期限结束前修改运行的数据库实例等级的任何属性，该数据库实例的小时使用费用将恢复为按需小时费用。如果稍后修改运行的数据库实例的属性以与原始预 留的属性相匹配，或按与原始预留相同的属性创建新数据库实例，在预留期限结束前将应用您的预留价格。

### 问：Amazon RDS 存储的硬件配置是什么？

Amazon RDS 的数据库和日志存储采用 EBS 卷。根据所请求存储的容量，Amazon RDS 自动将多个 EBS 卷分成条状以增强 IOPS 性能。对于 MySQL 和 Oracle 中现有的数据库实例，在扩展存储时，可以看到部分 I/O 的容量有所改进。您可以使用 [AWS 管理控制台](https://console.aws.amazon.com/)、[rds-modify-db-instance command](http://docs.aws.amazon.com/AmazonRDS/latest/CommandLineReference/CLIReference-cmd-ModifyDBInstance.html) 或 [ModifyDBInstance API](http://docs.amazonwebservices.com/AmazonRDS/2010-07-28/APIReference/index.html?API_ModifyDBInstance.html) 来扩展为数据库实例分配的存储容量。

不过，对于 SQL Server，由于连接到 Windows Server 环境的条状存储的扩展限制，Amazon RDS 当前不支持增加存储。

### 问：什么是 Amazon RDS 通用型 (SSD) 存储？

Amazon RDS 通用型 (SSD) 存储适用于拥有适度 I/O 请求的广泛数据库工作负载。凭借 3 IOPS/GB 的基准以及激增至 3000 IOPS 的能力，此存储方案将提供可预测的性能，以满足大多数应用程序的需求。

### 问：什么是 Amazon RDS 预配置 IOPS (SSD) 存储？

Amazon RDS 预配置 IOPS (SSD) 存储是支持 SSD 的存储方案，旨在提供快速、可预测和一致的 I/O 性能。凭借 Amazon RDS 预配置 IOPS (SSD) 存储，您可以在创建数据库实例时指定 IOPS 数量，而 Amazon RDS 可以为数据库实例的生命周期配置 IOPS 数量。Amazon RDS 预配置 IOPS (SSD) 存储经过优化，适合 I/O 密集型、事务处理型 (OLTP) 数据库工作负载。有关更多详情，请参阅 [Amazon RDS User Guide](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)。

### 问：什么是 Amazon RDS 磁性存储？

Amazon RDS 磁性存储原名为标准存储，适用于数据访问频率较低的小型数据库工作负载。

### 问：我如何在众多的 Amazon RDS 存储类型中进行选择？

选择最适合您工作负载的存储类型。

* 高性能 OLTP 工作负载：Amazon RDS 预配置 IOPS (SSD) 存储
* 具有适度 I/O 要求的数据库工作负载：Amazon RDS 通用型 (SSD) 存储
* 具有低频率 I/O 的小型数据库工作负载：Amazon RDS 磁性存储

### 问：自动备份和数据库快照之间有何差异？

Amazon RDS 提供两种备份和还原数据库实例自动备份和数据库快照（数据库快照）的不同方法。

通过 Amazon RDS 的自动备份功能，可以实现数据库实例的时间点恢复。为数据库实例打开自动备份时，Amazon RDS 将自动对数据执行全天快照（在首选的备份窗口期间）并获取事务日志（如果对数据库实例进行了更新）。启动时间点恢复时，事务日志将应用到最合适的每日备 份，以便将数据库实例还原到您请求的特定时间。Amazon RDS 可在用户指定的限定时间段（称为“保留期”）内保留数据库实例备份，默认情况下是一天，最长可以设置为 35 天。在保留期内，您可以启动时间点还原并指定任何秒数，最多为最近可还原的时间。您可以使用 DescribeDBInstances API 返回到数据库实例最近可还原的时间，通常在最后五分钟以内。此外，您可以在 [AWS 管理控制台](https://console.aws.amazon.com/)中选择数据库实例，并查看控制台下侧面板的“描述”选项卡，了解该数据库实例最近可还原的时间。

数据库快照由用户启动，让您能够按所需的任意频率在已知状态备份数据库实例，然后随时还原到该特定的状态。数据库快照可以使用 [AWS 管理控制台](https://console.aws.amazon.com/)或 CreateDBSnapshot API 创建，并将一直保留，直到您使用控制台或 DeleteDBSnapshot API 显式将其删除。

您可以使用 Amazon RDS 为实现自动备份而执行的快照来进行复制（使用 AWS 控制台或 rds-copy-db-snapshot 命令）或用于快照还原功能。您可以使用“自动”快照类型来确定它们。此外，您可以查看“快照创建时间”字段来确定拍摄快照的时间。另外，“自动”快照的标 识符中也包含快照拍摄的时间（UTC 形式）。

请注意：执行还原到某个时间点操作或从数据库快照执行还原操作时，将以新的终端节点创建一个新数据库实例（如果需要，可以使用 AWS 管理控制台或 DeleteDBInstance API 删除旧数据库实例）。这样，将使您能够从特定数据库快照或时间点创建多个数据库实例。

问：我的自动备份和数据库快照存储在哪里？**我可以怎样保留它们？**

Amazon RDS 数据库快照和自动备份存储在 S3 中。

### 问：是否可以将 VPC 内的现有数据库实例移到 VPC 外？

当前，不支持直接将数据库实例从 VPC 内部迁移到外部。出于安全考虑，无法将 VPC 内数据库实例的数据库快照还原到 VPC 外部。同样，也无法执行“还原到时间点”功能。如果需要将数据库实例从 VPC 内部移到外部，您需要将数据从 VPC 中的源数据库实例导出到 VPC 外部署的目标数据库实例。

### 问：要确保我的应用程序可以访问 VPC 中的数据库实例，我应该注意什么？

**您需要负责修改 VPC 中的路由表和网络 ACL，以确保能够从 VPC 中的客户端实例访问您的数据库实例。**

**对于多可用区域部署，在故障转移后，您的客户端 EC2 实例和 RDS 数据库实例可能位于不同的可用区域。您需要配置网络 ACL，以确保能够跨可用区域进行通信。**

### 问：是否可以使用 SSL 对我的应用程序和数据库实例之间的连接加密？

是的，此选项当前支持 MySQL、MariaDB、SQL Server、PostgreSQL、和 Oracle 引擎。

Amazon RDS 会为每个数据库实例生成一个 SSL 证书。建立加密连接后，在传输时将对数据库实例和应用程序之间传输的数据进行加密。

虽然 SSL 有安全优势，但应注意 SSL 加密操作需使用大量计算操作，可能会加大数据库连接延迟。Amazon RDS 中的 SSL 支持用来对应用程序和数据库实例之间的连接加密；不是应依赖于数据库实例本身的身份验证。

### 问：我能否加密 Amazon RDS 数据库上的静态数据？

Amazon RDS 使用您通过 [AWS Key Management Service (KMS)](https://aws.amazon.com/cn/kms/) 管理的密钥来支持所有数据库引擎的静态加密。在运行了 Amazon RDS 加密的数据库实例中，将加密基础存储中静态存储的数据，方法与其自动化备份、只读副本和快照一样。加密和解密操作的处理都是透明的。有关将 KMS 与 Amazon RDS 一起使用的更多信息，请参阅“[Amazon RDS User's Guide](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html)”。

问：什么是数据库参数组？**它们可提供什么帮助？**

数据库参数组（数据库参数组）就像是引擎配置值“容器”，这些值可应用于一个或多个数据库实例。如果创建的数据库实例未指定数 据库参数组，将使用默认的数据库参数组。该默认组包含针对您运行的数据库实例进行优化的引擎默认值和 Amazon RDS 系统默认值。不过，如果希望数据库实例以您自定义的引擎配置值运行，可以轻松地创建一个新数据库参数组，修改所需的参数并修改数据库实例以使用新数据库参 数组。建立关联后，使用特定数据库参数组的所有数据库实例都将获得该数据库参数组的所有参数更新。有关配置数据库参数组的更多信息，

问：Amazon RDS 支持哪些类型的副本？**何时应使用各种副本？**

Amazon RDS 提供两种不同的复制选项以满足不同的用途。

如果您希望用复制来增强数据库可用性，同时保护最新数据库更新以免意外中断，可考虑以多可用区域部署模式运行数据库实例。在创 建或修改数据库实例以便作为多可用区域部署运行时，Amazon RDS 将在不同的可用区域（物理位置分隔的独立基础设施）自动预配置和管理一个“备用”副本。如果遇到计划的数据库维护、数据库实例故障或可用区域故 障，Amazon RDS 将自动故障转移到备用副本，以便没有管理干预也能很快恢复数据库操作。多可用区域部署采用同步复制，使主副本和备用副本上的数据库写入并行执行，以便备用 副本在出现故障转移时保持最新状态。虽然多可用区域部署技术实施在出现故障时可以使数据持久性最大化，但在读取操作中会阻止直接访问或使用备用副本。多可 用区部署提供容错功能，使其自然而然适合生产环境；有关多可用区部署的详细信息，请访问[常见问题部分](http://aws.amazon.com/rds/faqs/#multi-az-deployments)。

MySQL、Oracle、PostgreSQL 和 SQL Server 数据库引擎均支持多可用区域部署。SQL Server 的多可用区部署当前可用于美国东部（北弗吉尼亚州）、美国西部（俄勒冈州）以及欧洲（都柏林）AWS 地区。

为帮助您扩展并超越单个数据库实例的容量限制，以处理高读取量的工作负载，Amazon RDS 提供只读副本。您可以使用 AWS 管理控制台或 CreateDBInstanceReadReplica API 为给定的源数据库实例创建只读副本。创建只读副本后，源数据库实例中的数据库更新将会填充到只读副本。您可以为给定的源数据库实例创建多个只读副本，并在 它们当中分配应用程序的读取流量。

Amazon RDS for MySQL 和 PostgreSQL 支持只读副本。与多可用区部署不同，这些引擎的只读副本利用各自的内置复制技术，且受其优势和局限约束。特别是，对源数据库实例进行更新后，更新会应用到 读取副本（“异步”复制），但复制滞后性可能会有很大差别。这意味着，如果源数据库实例出现意外故障，最近对标准（非多可用区域部署）源数据库实例进行的 数据库更新可能不会存在于关联的读取副本中。因此，读取副本不能提供与多可用区域部署相同的数据持久性优势。尽管只读副本具备一些读取可用性优势，但它们 对写入可用性没有改善。

您可以将多可用区部署和读取副本相互结合，以获得两者互补的优势。您可以轻松地将给定的多可用区域部署指定为读取副本的源数据库实例。这样，即可获得多可用区域部署的数据持久性和可用性优势，以及读取副本的读取扩展优势。

### 问：以多可用区域部署模式运行数据库实例意味着什么？

创建或修改数据库实例以多可用区域部署模式运行后，Amazon RDS 将自动在不同的可用区域预配置和维护同步“备用”副本。对数据库实例的更新将同步复制到可用区域的备用副本中，以保持同步并保护最新的数据库更新，以防数 据库实例出现故障。如果遇到特定类型的意外维护或很少出现的数据库实例故障或可用区域故障，Amazon RDS 将自动故障转移到备用副本，以便在提示备用副本后尽快恢复数据库写入和读取操作。由于数据库实例的名称记录相同，所以应用程序无需手动管理干预即可恢复数 据库操作。借助多可用区域部署，可以透明地进行复制：无需与备用副本交互，而且它不会用来服务于读取流量。如果您正在使用适用于 MySQL 的 Amazon RDS 并希望扩展单一数据库实例读取流量的容量限制，可以部署一个或多个[读取副本](https://aws.amazon.com/cn/rds/faqs/#87)。

### 问：在多可用区域部署环境中，“主”和“备用”指什么？

以多可用区域部署模式运行数据库实例时，“主”副本服务于数据库写入和读取操作。此外，Amazon RDS 会在场景后预配置和维护“备用”副本，它是主副本的最新副本。在故障转移情况下，会“提示”备用副本。故障转移后，备用副本将成为主副本，并接受数据库操 作。在提示前的任何时候，无需与备用副本直接交互（例如，用于读取操作）。如果您有兴趣扩展读取流量，以突破单个数据库实例的流量限制，请参阅[读取副本](https://aws.amazon.com/cn/rds/faqs/#87)的相关常见问题。

### 问：多可用区域部署有哪些优势？

以多可用区域部署模式运行数据库实例的主要优势是可增强数据库持久性和可用性。多可用区域部署提供的可用性增强和容错功能，使其自然而然成为生产环境的理想之选。

以多可用区域部署模式运行数据库实例，在遇到罕见的数据库组件故障或某个可用区域可用性损失的情况下可确保数据安全。例如，如 果主副本中的存储卷出现故障，Amazon RDS 将自动启动故障转移到备用副本，在此您的所有数据库更新完整无缺。相对于单一可用区域的标准部署，这种方式提供更长的数据持久性，否则将需要用户启动还原 操作且最近可还原时间（通常在最后五分钟内）之后进行的更新将不可用。

此外，以多可用区域部署模式运行时，还可获得增强数据库可用性的优势。如果发生可用区域故障或数据库实例故障，可用性影响将仅 限于完成自动故障转移的时间。多可用区域部署的可用性优势还可延伸到计划的维护操作。例如，对于自动备份，由于从备用副本进行备份，所以在首选的备份窗口 期间不会再暂停主副本中的 I/O 活动。至于补丁或数据库实例等级扩展，这些操作在自动故障转移前会首先在备用副本执行。因此，可用性影响将仅限于完成自动切换所需的时间。

以多可用区域部署模式运行数据库实例的另一潜在优势是，数据库实例故障转移自动执行，无需进行管理。在 Amazon RDS 环境中，这意味着出现可用区域故障或数据库实例故障时，无需监控数据库实例事件及启动手动数据库实例恢复（通过 RestoreDBInstanceToPointInTime 或 RestoreDBInstanceFromSnapshot API）。

### 问：以多可用区域部署模式运行我的数据库实例是否会影响性能？

您可以看到，由于代您执行同步数据复制，所以相对于单一可用区域的标准数据库实例部署，延迟有所提升。

### 问：以多可用区域部署模式运行我的数据库实例时，是否可使用备用副本来执行读取或写入操作？

不能，备用副本不能用于读取请求。多可用区域部署旨在增强数据库可用性和持久性，而非针对读取扩展优势。因此，该功能在主副本 和备用副本之间采用同步复制。我们的实施可确保主副本和备用副本一直处于同步状态，但不能使用备用副本执行读取或写入操作。如果您对读取扩展解决方案感兴 趣，请参见[读取副本](https://aws.amazon.com/cn/rds/faqs/#87)上的常见问题。

### 问：当我将 RDS 实例从单可用区转换为多可用区时，会发生什么情况？

对于 RDS MySQL、MariaDB、PostgreSQL 和 Oracle 数据库引擎，当您选择将 RDS 实例从单可用区转换为多可用区时，会发生以下情况：

* 拍摄主实例的快照
* 在不同的可用区，从该快照创建新的备用实例
* 在主实例和备用实例之间配置同步复制

因此，在实例从单可用区转换为多可用区时，不会出现停机时间。

### 问：哪种事件会导致 Amazon RDS 将故障转移启动到热备用副本？

Amazon RDS 可检测多可用区域部署中最常见的故障并自动从中恢复过来，这样您可在无管理干预的情况下尽快恢复数据库操作。如果发生以下任何一种情况，Amazon RDS 将自动执行故障转移：

* 主可用区域的可用性受损
* 主区域的网络连接受损
* 主区域的计算设备出现故障
* 主区域的存储故障

注意：为了获得更强的可用性，对多可用区域部署启动诸如数据库实例扩展或系统升级之类的操作时，如操作系统安装补丁程序，这些 操作首先会应用于备用，之后才应用于自动故障转移。因此，可用性影响将仅限于完成自动切换所需的时间。请注意，Amazon RDS 多可用区域部署不会自动转移来响应某些数据库操作，如长时间运行查询、死锁或数据库崩溃错误。

### 问：在多可用区域部署中如何应用数据库快照和自动备份？

您可以按照在单一可用区域或多可用区域部署中运行标准部署的相同方式与自动备份和数据库快照功能交互。如果您正在运行多可用区 域部署，将自动从备用副本执行自动备份和数据库快照，以免主副本中的 I/O 暂停。请注意，在备份单一可用区域和多可用区域部署时，您可能会经历更长时间的 I/O 延迟（一般持续几分钟）。

多可用区域部署与标准、单一可用区域部署的还原操作启动方式也完全相同（时间点还原或从数据库快照还原）。可以使用 RestoreDBInstanceFromSnapshot 或 RestoreDBInstanceToPointInTime API 创建新数据库实例部署。无论在标准部署还是多可用区域部署中启动源备份，这些新数据库实例部署都可能是标准或多可用区域模式。

### 问：以只读副本方式运行数据库实例意味着什么？

借助只读副本，用户能够轻松地利用受支持引擎的内置复制功能灵活扩展并超越单一数据库实例的容量限制，以处理大量读取数据库工 作负载。在 AWS 管理控制台中单击几下鼠标或使用 CreateDBInstanceReadReplica API 即可创建只读副本。创建只读副本后，将使用受支持引擎的本机异步复制功能复制源数据库实例的数据库更新信息。您可以为给定的源数据库实例创建多个只读副 本，并在它们当中分配应用程序的读取流量。由于只读副本利用受支持引擎的内置复制功能，所以它们受其优势和局限约束。特别是，对源数据库实例进行更新后， 更新将应用到读取副本，但复制滞后性可能会有很大差别。可以将读取副本与多可用区域部署关联起来，从而获得读取扩展优势，同时实现[多可用区域部署](https://aws.amazon.com/cn/rds/faqs/#36)提供的增强的数据库写入可用性和数据持久性。

### 问：何时应考虑使用 Amazon RDS 只读副本？

在很多情况下，为给定的源数据库实例部署一个或多个读取副本可能比较明智。部署读取副本的常见原因包括：

* 扩展用于执行大量读取数据库工作负载的单一数据库实例的计算资源或 I/O 容量。这样，过多的读取流量将被引导到一个或多个读取副本。
* 当源数据库实例不可用时，为读取流量提供服务。如果您的源数据库实例无法处理 I/O 请求（例如，由于备份或计划维护而暂停 I/O），可以将读取流量引导到读取副本。对于这种使用案例，请注意由于源数据库实例不可用，读取副本中的数据可能处于“静态”。
* 业务报告或数据仓库情况；您可能希望针对读取副本运行业务报告，而非主副本的生产数据库实例。

### 问：如何为指定的数据库实例部署只读副本？

使用标准的 CreateDBInstanceReadReplica API 或在 Amazon RDS 管理控制台中单击几下鼠标即可很快创建一个读取副本。创建读取副本后，可以通过指定 SourceDBInstanceIdentifier 将其标识为读取副本。 SourceDBInstanceIdentifier 是您要复制的“源”数据库实例的数据库实例标示符。同标准数据库实例一样，您也可以指定可用区域、数据库实例等级和首选维护窗口。只读副本的引擎版本（例 如，PostgreSQL 9.3.5）和存储分配均继承自源数据库实例。启动创建读取副本时，Amazon RDS 将对源数据库实例拍摄快照，并开始复制。因此，在拍摄快照时，您的源数据库实例上的 I/O 可能会短暂性停止。通常，I/O 暂停会按顺序持续一分钟时间；如果源数据库实例为多可用区域部署模式，则可以避免这种状况（对于多可用区域部署，从备用副本拍摄快照）。此 外，Amazon RDS 当前正在进行优化（很快即将发布），因此如果您在 30 分钟的窗口内创建多个读取副本，所有副本都将使用相同的源快照以降低 I/O 影响（每个读取副本将在创建后开始“追踪”复制）。

删除 Amazon RDS 读取副本同创建一样简单；只需使用 Amazon RDS 管理控制台或调用 DeleteDBInstance API 即可（为您要删除的读取副本指定 DBInstanceIdentifier）。

在请求创建读取副本时，还需要考虑下面一些事项：

* 如果您使用的是非事务性引擎（如 MyISAM），需要执行下列步骤来成功设置读取副本。执行这些步骤，是为了确保读取副本包含一致的数据副本。请注意，如果您的所有表使用的都是事务性引 擎（如 InnoDB），则无需执行这些步骤。1. 停止非事务性表中的所有 DML 和 DDL 操作，等待它们完成操作。SELECT 语句可以继续运行。2. 刷新和锁定这些表。3. 使用 CreateDBInstanceReadReplica API 创建读取副本。 4. 使用 DescribeDBInstances API 检查副本的创建进度。 当副本可用后，对表解锁并恢复正常的数据库操作。
* 如果源 RDS 实例中有任何运行时间较长的事务，请等待它们完成，再请求从该源创建读取副本。

### 问：我可以为给定的源数据库实例创建多少个只读副本？

目前，您可以使用 Amazon RDS for MySQL 和 PostgreSQL 为一个给定的源数据库实例最多创建五个 (5) 只读副本。

### 问：我能否在不同于源数据库实例的 AWS 区域中创建只读副本？

适用于 MySQL 和 PostgreSQL 的 Amazon RDS 支持跨区域只读副本。

### 问：我能否使用只读副本来增强数据库写入可用性或保护源数据库实例中的数据以防出现故障？

如果您希望使用复制来增强数据库写入可用性以及保护最近的数据库更新以防出现各种故障，我们建议您以多可用区部署模式运行数据 库实例。借助采用支持引擎本机异步复制公司的 Amazon RDS 只读副本，只读副本会在源数据库实例中执行数据库写入操作后也发生数据库写入，而且这种复制“滞后性”可能存在很大差别。相比之下，多可用区域部署采用的 副本属于同步复制，意味着主副本和备用副本上的数据库写入会并发执行。这样可保护最新的数据库更新，因为在出现故障转移时，它们需要在备用副本中可用。此 外，使用多可用区域部署，可完全托管复制操作。Amazon RDS 将自动监控数据库实例的故障条件或可用区域故障，并在出现中断时启动到备用副本的自动故障转移。

### 问：我能否将我的 Amazon RDS 只读副本本身放入多可用区？

Amazon RDS for MySQL 和 PostgreSQL 目前不支持此功能。

### 问：如果我的只读副本使用多可用区域部署的数据库实例作为源，在发生多可用区域故障转移时，会出现什么状况？

对于多可用区故障转移，所有关联和可用的只读副本在故障转移完成后将自动恢复复制（获取最新提升的主副本的更新）。

### 问：我的 Amazon RDS for MySQL 只读副本在多可用区故障转移后呈现“阻塞”状态，无法获取或应用源数据库实例的更新。我应该怎么办？

有些情况下，您会发现在多可用区故障转移后，Amazon RDS for MySQL 只读副本无法接收或应用其源多可用区数据库实例的更新。这是因为，有些 MySQL 二进制日志事件在故障转移时未更新到磁盘。故障转移后，读取副本可能会获取其缺少的源的二进制日志。[下面](http://dev.mysql.com/doc/refman/5.1/en/binary-log.html)的 MySQL 文档中描述了崩溃时缺失的 MySQL 二进制日志。

底部一段与本问题尤其相关，其中描述了 MySQL sync-binlog 参数。该参数控制 MySQL 二进制日志更新到磁盘的方式，以及使用 InnoDB 时，如何同步保留二进制日志和 InnoDB 日志。

要解决当前的问题，您需要删除该读取副本并创建一个新读取副本来替换它。要避免将来再出现此问题，设置 sync-binlog=1 可大大降低这种可能性，因为在崩溃/故障转移情况下可能会丢失读取副本所需的 MySQL 二进制日志。如 MySQL 文档所述，即使这样也不能完全解决该问题。要进一步降低出现此问题的可能性，请设置 innodb\_support\_xa=1。请注意，设置这些变量可能会影响性能。由于 sync\_binlog 和 innodb\_support\_xa 均为动态变量，所以如果您觉得性能影响过大，可以在不中断的情况下重设这些变量。

在源多可用区域故障转移后，它们将成为性能和改进读取副本自动重新同步之间的最终选择。Amazon RDS 读取副本的优势之一是，在出现同步问题时，可通过删除和重新创建副本快速重新进行实例化。因此，如果手动删除同步读取副本和重新创建它们可以满足需求，则 不必再通过设置 sync-binlog 和/或 innodb\_support\_xa 来提高性能。

### 问：我的只读副本是否只能接受数据库读取操作？

读取副本旨在服务于读取流量。不过，在某些使用案例中，高级用户可能希望针对读取副本完成数据定义语言 (DDL) SQL 语句。例如，这些情况可能包括向用于业务报告的只读副本添加数据库索引，而不向对应的源数据库实例添加相同的索引。

Amazon RDS for MySQL 可配置为允许针对只读副本的 DDL SQL 语句。如果希望启用读取给定只读副本之外的操作，则需要修改该只读副本的有效数据库参数组，将“read\_only”参数设置为“0”。

Amazon RDS for PostgreSQL 目前不支持针对只读副本的 DDL SQL 语句的执行。

### 问：是否可以对只读副本拍摄数据库快照或执行自动备份？

不可以。如果您希望通过从读取副本（而非源数据库实例）执行备份而增强数据库写入可用性，可以采用多可用区域部署方式运行数据库实例来实现相同的目标。 然后，将继承多可用区域备用副本的备份，以尽可能降低对可用性的影响。

问：如何删除只读副本？

您在 AWS 管理控制台中单击几下鼠标或将数据库实例标识符传送到 DeleteDBInstance API，即可轻松地删除只读副本。

即使在已删除相应的源数据库实例后，Amazon RDS for MySQL 只读副本仍然保持有效并可继续接受读取流量。如果您需要同时删除只读副本和源数据库实例，则必须使用 DeleteDBInstance API 或 AWS 管理控制台明确执行此操作。

问：如果源数据库实例被删除，只读副本是否会自动删除？

如果您删除了一个具有只读副本的 Amazon RDS for PostgreSQL 数据库实例，则所有的只读副本都将被提升为独立的数据库实例，并将能够接受读取和写入流量。新提升的数据库实例将彼此独立地运行。如果您需要同时删除这些 数据库实例和源数据库实例，则必须使用 DeleteDBInstance API 或 AWS 管理控制台明确执行此操作。

### 问：我是否可以直接访问数据库实例的事件日志来管理自己的复制？

Amazon RDS for MySQL 目前不提供访问数据库实例的二进制日志的权限。同样地，Amazon RDS for PostgreSQL 目前也不提供访问数据库实例 WAL 文件的权限。

问：只读副本的成本是多少？**如何计算记账周期？**

只读副本按标准数据库实例进行计费，且费率相同。有关数据库实例账单的更多信息，请单击此处访问[常见问题](https://aws.amazon.com/cn/rds/faqs/#15)。如同标准数据库实例，只读副本的每“数据库实例小时”费用取决于只读副本的数据库实例等级 – 有关最新的定价信息，请参见 Amazon RDS [详细信息页面](https://aws.amazon.com/rds/pricing/)。在源数据库实例和读取副本之间复制数据，产生的数据传输不收取费用。

读取副本的账单周期从成功创建读取副本后开始（即当列出的状态为“有效”时）。读取副本将一直按标准 Amazon RDS 数据库实例小时费用计费，直到您发布命令将其删除为止

### 问：Enhanced Monitoring 支持哪些实例类型？

答：Enhanced Monitoring 支持除 t1.micro 和 m1.small 以外的所有实例类型。该软件占用少量 CPU、内存和 I/O 即可实现常规监控；对于中型或大型实例，我们建议切换至更高的粒度。Enhanced Monitoring 的默认设置是“off”，您可以选择让其保持禁用状态，也可以在启用时修改粒度。

### 问：如何将 Enhanced Monitoring 与我当前使用的工具集成？

答：RDS Enhanced Monitoring 提供了一系列将以 JSON 有效负载形式发送到您的 CloudWatch Logs 账户的指标。JSON 有效负载会按照上次为 RDS 实例配置的粒度进行发送。

### RedShift

Amazon Redshift 是一种快速、强大且完全托管的 PB 级[云](https://aws.amazon.com/cn/what-is-cloud-computing/)中数据仓库服务。客户可以以每小时 0.25 USD 的价格从小做起，无需订立长期合约或预付费，然后以每年每 TB 1000 USD 的价格再扩展到 1PB 或以上，这个费用比大多数其他数据仓库解决方案成本的十分之一还要低。

传统的数据仓库需要相当数量的时间和资源来进行管理，尤其是大型数据集。 另外，与内部部署型数据仓库的建立、维护及日益增长的自我管理相关的财务成本也非常之高。Amazon Redshift 不仅大大降低了数据仓库的成本，而且还能轻而易举地对大量数据进行快速分析。

Amazon Redshift 为您提供利用基于 SQL 的常用客户端及商业智能 (BI) 工具通过标准的 ODBC 和 JDBC 连接对结构化数据进行快速查询的功能。查询为多个物理资源之间的分布式并行查询。您在 AWS 管理控制台中点击几次或调用一个 API 即可轻松对 Redshift 数据仓库进行扩展或缩减。Amazon Redshift 自动修补数据仓库并将其备份，并按照用户定义的保留期存储备份。Amazon Redshift 利用复制和连续备份来提高可用性并改善数据持久性，从而能从组件或节点故障中自动恢复。此外，为了保护您的中转数据和静态数据，Amazon Redshift 支持 Amazon 虚拟私有云 (Amazon VPC)、SSL 和 AES-256 加密和硬件安全模块 (HSM)。

与所有 Amazon Web 服务服务相同，它无需预先投资，而且您只需为您使用的资源付费。Amazon Redshift 根据您的使用量进行收费。甚至可以免费试用 [Amazon Redshift。](https://aws.amazon.com/cn/redshift/partners/)

问：Amazon Redshift 可代我管理哪些内容？  
  
Amazon Redshift 管理数据仓库的设置、运行及扩展所必须的工作，从基础结构容量的预配置到当前管理任务（如备份和修补）的自动化。Amazon Redshift 自动监控节点和驱动器，帮助您从故障中恢复。

问：与最传统的数据仓库存储及分析用数据库相比，Amazon Redshift 的性能如何？  
  
Amazon Redshift 使用各种创新技术，与传统的数据仓库仓储及分析用数据库相比，其性能提高将近十倍：

* *列式数据存储*：Amazon Redshift 以列组织数据，并非以一系列的行来存储数据。与适用于事务处理的基于行的系统不同，基于列的系统适用于数据仓库存储及分析，在此系统下，查询经常涉及到对 大型数据集进行聚合。由于仅对涉及查询的列进行处理，且列式数据顺序存储在存储介质上，故基于列的系统所需的 I/O 要少得多，从而显著提高了查询性能。
* *高级压缩*：与基于行的数据存储相比，列式数据存储可进行更大程度的压缩，因为类似的数据是按顺序存储在硬盘 上。Amazon Redshift 拥有多种压缩技术，与传统的关系数据存储相比，经常可进行很大程度的压缩。此外，与传统的关系数据库系统相比，Amazon Redshift 不需要索引或具体化视图，因此使用的空间较少。将数据加载到空表中时，Amazon Redshift 自动对您的数据进行采样并选择最合适的压缩方案。
* *大规模并行处理 (MPP)*：Amazon Redshift 在所有节点之间自动分配数据及查询负载。Amazon Redshift 可轻松将节点添加至您的数据仓库，而且随着您的数据仓库规模的扩大，仍能维持快速的查询性能。

问：我如何创建一个 Amazon Redshift 数据仓库集群？  
  
您可用 [AWS 管理控制台](https://aws.amazon.com/cn/console/) 或 [Amazon Redshift API轻松创建一个 Amazon Redshift 数据仓库集群。](http://docs.aws.amazon.com/redshift/latest/APIReference/Welcome.html)您可以从单一节点 160GB 数据仓库开始，然后在 [AWS 控制台](https://aws.amazon.com/cn/console/)中单击几下或进行一次 API 调用，一路扩展到 1 PB 或更大。

单节点配置使您能够开始经济快速地使用 Amazon Redshift，而且随着您的需求的增长，单节点配置可扩展为多节点配置。多节点配置需要一个领导节点来管理客户端的连接并接收查询，以及两个计算节点 来存储数据并执行查询和计算。自动为您配置领导节点，您无需为其付费。

仅需指定您的首选可用区（可选项）、节点数量、节点类型、 主机名称和密码、安全组、您对备份保留期的首选项及其他系统设置。一旦您已选定您的理想配置，Amazon Redshift 将预配置所需的资源并建立您的数据仓库集群。

问：领导节点和计算节点分别起什么作用？  
  
领导节点接收来自客户端应用程序的查询，分析查询并制定执行计划，执行计划是对查询进行处理的一套有序步骤。然后领导节点和计算节点协调这些计划的并行执行，聚合来自这些节点的中间结果，并将这些结果最终返回至客户端应用程序。

计算节点执行执行计划所规定的步骤，并在它们之间传输数据，对这些查询进行服务。中间结果被送回至客户端应用程序之前，它们被送回至领导节点进行聚合。

**每个计算节点的建议数据量是多少？**  
  
您可以使用密集存储 (DS) 节点或密集计算节点 (DC) 创建集群。通过密集存储节点，您可以以非常低的价格使用硬盘 (HDD) 创建超大型数据仓库。通过密集计算节点，您可以使用高速 CPU、大量的 RAM 和固态硬盘 (SSD) 创建性能极高的数据仓库。

密集存储 (DS) 节点以两种大小提供：超大型节点和八倍超大型节点。超大型节点 (XL) 有 3 个硬盘，总共为 2TB 的磁盘存储，而八倍超大型节点 (8XL) 有 24 个硬盘，总共为 16TB 磁盘存储。DS2.8XL 有 36 个 Intel Xeon E5-2676 v3 (Haswell) 虚拟内核和 244GiB RAM，DS2.XL 有 4 个 Intel Xeon E5-2676 v3 (Haswell) 虚拟内核和 31GiB RAM。请参阅定价页面了解更多详细信息。您可从每小时 0.85 USD 的单个超大型节点 2TB 数据仓库开始，然后扩展至 1 PB 或更大。您可按小时付费或使用预留实例定价，将价格降低到每年每 TB 不到 1 000 USD。

密集计算 (DC) 节点也具有两种规格。大型节点具有 160GB 的 SSD 存储、2 个 Intel Xeon E5-2670v2 (Ivy Bridge) 虚拟核心和 15GiB 的 RAM。八倍超大型节点是大型节点的 16 倍，具有 2.56TB 的 SSD 存储、32 个 Intel Xeon E5-2670v2 虚拟核心和 244GiB 的 RAM。您可从每小时 0.25 USD 的单个大型节点开始，然后一路扩展至 128 个 8XL 节点，从而具有 326TB 的 SSD 存储、3 200 个虚拟核心和 24TiB 的 RAM。

Amazon Redshift 的 MPP 架构意味着可以通过增加数据仓库集群中的节点数来提升性能。每个计算节点的最佳数据量取决于您的应用特点和您的查询性能需求。

Amazon Redshift 和 [Amazon RDS](https://aws.amazon.com/cn/rds/) 都让您能够在云中运行传统的关系数据库，同时转移数据库管理负载。客户既将 Amazon RDS 数据库用于联机事务处理 (OLTP) ，也将其用于报告和分析。Amazon Redshift 利用多节点的规模和资源并使用各种优化法，为传统数据库对大型数据集的分析及报告工作负荷提供了数量级改善。当您的数据及查询的复杂性增加时，或者，在您 要防止报告和分析处理对 OLTP 工作负荷造成干扰时，Amazon Redshift 提供优秀的外扩选项。

问：我什么时候使用 Amazon Redshift 或者 Amazon Elastic MapReduce (Amazon EMR)？  
  
Amazon Redshift 适用于您想持久保持的并用标准 SQL 和现有 BI 工具进行查询的大量结构化数据。[Amazon EMR](https://aws.amazon.com/cn/elasticmapreduce/) 适用于处理并转换非结构化或半结构化数据，以便将它们引入到 Amazon Redshift 中，对于相对短期的且并非为长期使用之目的而存储的数据集，它也是一个更好的选择。

仅按实际使用量收费，无最低费用或设置费用。您的计费依据为：

* *计算节点小时数* – 计算节点小时数是在计费期内运行的所有计算节点的小时总数。按照每小时每节点一个单位计费，因此一个持续运行一整个月的三节点数据仓库集群将产生 2 160 个实例小时。您无需为领导节点小时数付费；仅计算节点产生费用。
* *备份存储* – 备份存储是与数据仓库自动化及手工快照相关的存储。延长备份保留期或增加快照拍摄数量，将增加数据仓库所消耗的备份存储。对于已激活的数据仓库实例而言， 无需额外付费，即可获得最多 100% 预配置数据仓库存储的备份存储。例如，如果您有一个已激活的具有 2TB 本地实例存储的单节点 XL 数据仓库集群，那么我们将提供高达 2TB-月的备份存储而无需额外付费。超出预配置存储大小的备份存储以及在集群终止之后存储的备份按[标准 Amazon S3 费率](https://aws.amazon.com/cn/s3/pricing/)计费。
* *数据传输* – 传输到 Amazon VPC 之外的 Amazon Redshift 或从其中传出的数据不计费。传输到 [Amazon VPC](https://aws.amazon.com/cn/vpc/) 之中的 Redshift 的数据或从其中传出的数据按照标准 AWS 数据传输计费。

问：我能用 SQL ‘INSERT’ 语句加载数据吗？  
  
可以，用户可用 ODBC 或 JDBC 连接至 Amazon Redshift 并发出 'insert' SQL 命名以插入数据。请注意这会比使用 S3 或 DynamoDB 慢一些，因为那些方法将数据并行加载至每个节点，而 SQL 插入语句则通过单个领导节点加载数据。

问：如何将数据从我现有的 Amazon RDS、Amazon EMR、Amazon DynamoDB 及 Amazon EC2 数据源加载至 Amazon Redshift？  
  
可以使用 [COPY 命令](http://docs.aws.amazon.com/redshift/latest/dg/r_COPY.html)以平行方式将数据从 Amazon EMR、Amazon DynamoDB 或任何启用了 SSH 的主机直接加载到 Amazon Redshift。不仅如此，许多 [ETL 公司](https://aws.amazon.com/cn/redshift/partners/)还对 Amazon Redshift 进行认证以使用其工具，同时我们提供一个电话号码帮助您使用[免费试用](https://aws.amazon.com/cn/redshift/partners/)开始加载数据。最后，[AWS Data Pipeline](https://aws.amazon.com/cn/datapipeline/) 提供一个从各种 AWS 数据源加载数据的高性能、可靠且容错的解决方案。您可用 AWS Data Pipeline 来指定数据源和理想的数据转换，然后执行一个预先写入的导入脚本，将您的数据加载到 Amazon Redshift 中。

问：Amazon Redshift 如何确保数据的安全性？  
  
Amazon Redshift 用行业标准加密技术进行加密并确保您的数据在中转过程及静态期间的安全性。 为了在中转期间确保数据安全性，Amazon Redshift 支持客户端应用程序及 Redshift 数据仓库集群之间的 SSL 使能型连接。为了在静态期间确保数据安全性，Amazon Redshift 用硬件加速型 AES-256 在将每个数据块写入硬盘之时对其进行加密。此过程以低等级形式发生在 I/O 子系统中，它对写入硬盘的一切数据进行加密，包括中间查询结果。数据块按原样进行备份，这意味着备份也进行了加密。

问：我能直接访问 Amazon Redshift 计算节点吗？  
  
不能。您的 Amazon Redshift 计算节点处于私有网络空间中，仅能从数据仓库集群的领导节点对其进行访问。这就为您的数据安全性提供了另外一层保护。

问：如果一个节点上的驱动器发生故障，那么对数据仓库集群的可用性和持久性有何影响？  
  
某个驱动器发生故障时，Amazon Redshift 数据仓库集群将仍然可供使用，不过您会发现某些查询的性能略有下降。某个驱动器发生故障时，Amazon Redshift 将透明地使用那个节点内其他驱动器上存储的数据副本。此外，Amazon Redshift 将力图把您的数据转移到一个健康的驱动器，或者在转移无法完成时，替换您的节点。 单个节点集群不支持数据复制。若发生驱动故障，您需要根据 S3 上的快照还原集群。我们建议您至少为生产使用 2 个节点。

问：如果个别节点发生故障，那么对数据仓库集群可用性和数据持久性有何影响？  
  
Amazon Redshift 将自动检测并替换数据仓库集群中的故障节点。在配置替换节点并将其添加至数据库之前，数据仓库集群无法进行查询和更新。Amazon Redshift 将使替换节点立即可用，并首先从 S3 中加载您最频繁访问的数据，让您尽快恢复数据查询。 单个节点集群不支持数据复制。若发生驱动故障，您需要根据 S3 上的快照还原集群。我们建议您至少为生产使用 2 个节点。

问：如果数据仓库集群的可用区 (AZ) 出现故障，那么对数据仓库集群可用性和数据持久性有何影响？  
  
如果 Amazon Redshift 数据仓库集群的可用区无法使用，那么在 AZ 的电源及网络访问恢复之前，您将无法使用您的集群。数据仓库集群的数据是这样保留的：一旦 AZ 重新可供使用，那么您就能够开始使用 Amazon Redshift 数据仓库。此外，您也可选择将任何现有快照恢复到同一区域中的一个新 AZ 中。Amazon Redshift 将首先恢复您最频繁访问的数据，这样您就能尽快地恢复查询。

问：Amazon Redshift 支持 Multi-AZ 部署吗？  
  
当前 Amazon Redshift 仅支持单一可用区部署。通过将数据从同一组 Amazon S3 输入文件加载到各自 AZ 中的两个 Amazon Redshift 数据仓库集群中，您便可在多个 AZ 中运行数据仓库集群。此外，您也可将数据仓库集群从数据仓库集群快照恢复至不同的可用区。

问：Amazon Redshift 如何备份数据？  
  
在加载数据时，Amazon Redshift 复制数据仓库集群内的所有数据并将其连续备份至 S3。 Amazon Redshift 始终力图维持至少三份数据（计算节点上的正本数据、副本数据和 Amazon S3 上的备份数据）。Redshift 还能将您的快照异步复制到另一个地区的 S3 中进行灾难恢复。

问：我需要启用数据仓库集群备份，还是它会自动启用？  
  
默认情形下，Amazon Redshift 以一天的保留期启用数据仓库集群自动化备份。免费备份存储被限制为数据仓库集群中节点上的总存储大小，并仅适用于已激活的数据仓库集群。例如，如果您有 8TB 的数据仓库总存储大小，那么我们将提供最多 8TB 的备份存储而不另外收费。如果您想将备份保留期延长为超过一天，那么您可用 [AWS 管理控制台](https://aws.amazon.com/cn/console/)或 [Amazon Redshift API](http://docs.aws.amazon.com/redshift/latest/APIReference/Welcome.html)来达到此目的。 有关自动快照的更多信息，请参阅 Amazon Redshift [Management Guide](http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html)。Amazon Redshift 仅备份已改变的数据，因此大多数快照仅占用少量的免费备份存储。

问：在扩展过程中数据仓库集群仍可供使用吗？  
  
对现有的数据仓库集群仍然可进行读操作，同时在扩展过程中将创建一个新的数据仓库集群。当新数据仓库集群准备好后，现有的数据仓库集群将暂时无法使用，同 时现有数据仓库集群的规范名称记录被翻转过来，指向新数据仓库集群。这段不可使用期间通常仅持续几分钟，将在数据仓库集群的维护时段期间出现，除非您指定 立即应用修改。Amazon Redshift 将数据从现有数据仓库集群并行转移至新数据仓库集群中的计算节点。这使您的操作能够尽快完成。

### Route 53

### 问：什么是 Amazon Route 53？

Amazon Route 53 提供高度可用且可扩展的域名系统 (DNS)、域名注册和运行状况检查 Web 服务。设计用于为开发人员和企业提供一种非常可靠且经济高效的方式，把名称（如 *example.com*）转换为计算机用于互相连接的数字 IP 地址（如 *192.0.2.1*），从而将最终用户路由到 Internet 应用程序。您可以将 DNS 与运行状况检查服务组合使用，路由流量到运行正常的终端节点，或者独立监控终端节点和/或对其提供警报。您还可以购买和管理域名（例如 *example.com*）， 并自动为域配置 DNS 设置。Route 53 高效地将用户请求连接到 AWS 中运行的基础设施，例如 Amazon EC2 实例、Elastic Load Balancing 负载均衡器或 Amazon S3 存储桶，还可以将用户转接到 AWS 外部的基础设施。

### 问：Amazon Route 53 上 DNS 设置更改的全球传播速度有多快？

正常情况下，Amazon Route 53 的设计可以在 60 秒内将您对 DNS 记录的更新传播到其授权 DNS 服务器的全球网络中。API 调用返回 *INSYNC* 状态列表时，即表示更改已成功完成全球传播。

请注意，缓存 DNS 解析器不在 Amazon Route 53 服务的控制范围内，它们将根据其生存时间 (TTL) 缓存您的资源记录集。更改的 *INSYNC* 或 *PENDING* 状态仅指示 Route 53 的授权 DNS 服务器的状态。

### 问：是否可以将我的主域顶点（example.com 与 www.example.com 相比）指向我的 Elastic Load Balancer？

可以。Amazon Route 53 提供一种称为“别名”记录的特殊记录类型，供您将顶级域名 (*example.com*) DNS 名称映射到 ELB DNS 名称（如 *elb1234.elb.amazonaws.com*）。 与 Amazon Elastic Load Balancer 关联的 IP 地址随时会由于大小扩展或软件更新而改变。Route 53 使用负载均衡器的一个或多个 IP 地址来响应别名记录的每个请求。对映射到 ELB 负载平衡器的别名记录的查询不收取费用。这些查询在 Amazon Route 53 使用率报告中列为“Intra-AWS-DNS-Queries”。

### 问：Amazon Route 53 是否支持加权轮询 (WRR)？

是。加权轮询可让您为资源记录集合分配权重，以便指定不同回复所服务的频率。您可能希望使用此功能来执行 A/B 测试，发送一小部分流量到进行了软件更改的服务器。例如，假设您向一个 DNS 名称关联了两个记录集合，其中一个的权重为 3，另一个的权重为 1。此情形中，75% 时间内 Route 53 将返回权重为 3 的记录集合，25% 时间内 Route 53 将返回权重为 1 的记录集合。权重可以是 0 到 255 范围内的任意数字。

### 问：Amazon Route 53 的 Geo DNS 功能是什么？

Route 53 Geo DNS 会根据请求发出的地理位置将其送至特定的终端节点，以此帮助调整负载平衡。Geo DNS 可以自定义本地化的内容，例如以正确的语言展示详情页面或限制将内容分配到已授权的市场。Geo DNS 通过一种可以预见而又易于管理的方式让您实现负载平衡，确保每一个终端用户地点始终路由到相同的终端节点。Geo DNS 提供三种地理粒度级别：洲、国家/地区和州/省，Geo DNS 还提供全球记录，当终端用户的地点与您创建的特定 Geo DNS 记录不匹配时，全球记录可在这种情况下发挥作用。您还可以将 Geo DNS 与其他路由类型（例如基于延迟的路由和 DNS 故障转移）进行组合，以实现多种低延迟的容错架构。关于如何配置各种路由类型的信息，请参见 [Amazon Route 53 文档](http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)。

### 问：基于延迟的路由和 Geo DNS 有何区别？

Geo DNS 根据请求的地理位置制定路由决策。某些情况下，地理位置是很好的延迟代理；但是某些情况下则不然。基于延迟的路由利用查看者网络和 AWS 数据中心之间的延迟测量值。这些测量值用于确定引导用户到达了哪个终端节点。

如果您的目标是尽量减少最终用户延迟，我们建议使用基于延迟的路由。如果您有合规性、本地化方面的要求，或者有需要从特定地理位置稳定路由至特定终端节点的其他使用案例，我们建议使用 Geo DNS。

### 问：私有 DNS 能不能在所有 AWS 区域中使用？

能。DNS 应答可以在与私有托管区域关联的每一个 VPC 中使用。注意，您需要保证每个区域中的所有 VPC 彼此相连，以便一个区域中的资源可以触及另一个区域中的资源。以下区域现已支持 Route 53 私有 DNS：美国东部（弗吉尼亚北部）、美国西部（加利福尼亚北部）、美国西部（俄勒冈）、亚太地区（孟买）、亚太地区（首尔）、亚太地区（新加坡）、亚太地 区（悉尼）、亚太地区（东京）、欧洲（法兰克福）、欧洲（爱尔兰）和南美洲（圣保罗）。

### 问：DNS 故障转移是否能支持将 Elastic Load Balancer (ELB) 用作终端节点?

可以，您可以为 Elastic Load Balancers (ELB) 配置 DNS 故障转移。若要启用一个 ELB 终端节点的 DNS 故障转移，请创建一个指向 ELB 的别名记录并将“Evaluate Target Health”参数设置为真。Route 53 会自动创建和管理您的 ELB 的运行状况检查。您无需创建您自己的 ELB Route 53 运行状况检查。您也不需要将您为 ELB 设置的资源记录与您自己的运行状况检查关联在一起，因为 Route 53 会代表您将它与 Route 53 管理的运行状况检查关联在一起。ELB 运行状况检查还会继承该 ELB 的后端实例的运行状况。

### 问：如果发生故障转移并且我拥有多个运行良好的终端节点，那么 Route 53 在决定从发生故障的终端节点发送流量时，是否会考虑运行状况良好的终端节点上的负载情况呢？

不会，Route 53 不会根据终端节点的负载或可用流量来决定路由目标。您将需要确保您的终端节点有可用容量，或这些终端节点具有扩展能力，以处理流向故障终端节点的流量。

### 问：当我的故障终端节点再次正常运行后，DNS 故障转移如何进行逆向转移呢？

在失败的终端节点通过您在创建运行状况检查时指定的连续运行状况检验观察的次数后（默认阈值为三次观察），Route 53 将自动恢复其 DNS 记录，并且流向该终端节点的流量将在无需您操作的情况下恢复。

### 问：Route 53 运行状况检查是否遵循 HTTP 重定向？

否。Route 53 运行状况检查将 HTTP 3xx 代码视为成功的响应，因此他们不会遵循重定向。这可能会导致字符串匹配运行状况检查出现异常结果。运行状况检查将在重定向的正文中搜索指定的字符串。由于 运行状况检查不遵循重定向，它永远不会将请求发送到重定向所指向的位置，因此也永远不会从该位置获得响应。对于字符串匹配运行状况检查，我们建议您不要使 用把运行状况检查指向某个将返回 HTTP 重定向的位置。

### 问：HTTPS 运行状况检查是否会验证终端节点的 SSL 证书？

不会，HTTPS 运行状况检查将测试是否能够通过 SSL 连接终端节点，以及终端节点是否会返回有效的 HTTP 响应代码。但是，它们不会验证终端节点返回的 SSL 证书。

### 问：如何使用 Amazon Route 53 测量应用程序终端节点的性能？

Amazon Route 53 运行状况检查包含可选的延迟测量功能，它会就终端节点响应请求所花的时间提供相关数据。当您启用延迟测量功能后，Amazon Route 53 运行状况检查将生成额外的 Amazon CloudWatch 指标，以显示 Amazon Route 53 运行状况检查程序建立连接并开始接收数据所需的时间。Amazon Route 53 将为执行 Amazon Route 53 运行状况检查的每个 AWS 区域提供一组单独的延迟指标。

### 问：对于指向 Amazon S3 网站存储段的别名记录，当我将“Evaluate Target Health”设置为“true”时，将会检查哪些项目的运行状况？

Amazon Route 53 在每个 AWS 区域执行 Amazon S3 服务本身的运行状况检查。当您在指向 Amazon S3 网站存储段的别名记录上启用“Evaluate Target Health”时，Amazon Route 53 会考虑存储段所处的 AWS 区域中的 Amazon S3 服务的运行状况。Amazon Route 53 不会检查特定的存储段是否存在或者是否包含有效网站内容；仅在存储段所处的 AWS 区域中没有可用的 Amazon S3 服务时，Amazon Route 53 才会故障转移至另一位置。

### S3

### 问：我可以存储多少数据？

您可以存储的总数据容量和对象个数不受限制。各个 Amazon S3 对象的大小范围可以从最小 0 字节到最大 5 TB。可在单个 PUT 中上传的最大数据元为 5 GB。对于大于 100 MB 的数据元，客户应该考虑使用[分段上传](http://docs.amazonwebservices.com/AmazonS3/latest/dev/UploadingObjects.html)功能。

### 问：Amazon S3 数据是如何组织的？

Amazon S3 是基于密钥的简单数据元存储。存储数据时，您应分配唯一数据元密钥，此后可使用该密钥来提取数据。密钥可以是任何字符串，可以模仿分层结构属性。

### 问：如何增加我可以预置的 Amazon S3 存储桶的数量？

默认情况下，客户最多可以为每个 AWS 账户预置 100 个存储桶。

### 问：Amazon S3 的费用是多少？

使用 Amazon S3，您只需可以按实际用量付费。没有最低收费。您可以使用 [AWS 简单月度成本结算器](http://calculator.s3.amazonaws.com/calc5.html)估算月度费用。

当我们的成本较低时，我们的收费也比较低。有些价格因 Amazon S3 地区而异，取决于您的存储段的位置。对于通过 COPY 请求在 Amazon S3 区域内部传输的数据，没有数据传输费用。通过 COPY 请求在区域间传输的数据按在 Amazon S3 详情页面的定价部分指定的费率收费。对于在同一区域内的 Amazon EC2 和 Amazon S3 之间传输的数据，或在 Amazon EC2 弗吉尼亚北部区域和 Amazon S3 美国东部（弗吉尼亚北部）区域之间传输的数据，没有数据传输费用。在 Amazon EC2 与所有其他区域的 Amazon S3 之间传输的数据（如在 Amazon EC2 加利福利亚北部和 Amazon S3 美国东部（弗吉尼亚北部）区域之间的传输）按在 Amazon S3 详情页面的定价部分指定的费率收费。

### 问：对存储在 Amazon S3 上的数据加密时，可以使用哪些选项？

您可以选择使用 SSE-S3、SSE-C、SSE-KMS 或客户端库（例如 [Amazon S3 加密客户端](http://docs.amazonwebservices.com/AWSJavaSDK/latest/javadoc/com/amazonaws/services/s3/AmazonS3EncryptionClient.html)）对数据进行加密。所有四个选项都可以将敏感的数据以静态方式存储在 Amazon S3 中。

SSE-S3 提供了一种集成式解决方案，Amazon 通过其使用多个安全层处理密钥管理和密钥保护问题。如果您希望 Amazon 管理您的密钥，您应该选择 SSE-S3。

SSE-C 让您能利用 Amazon S3 对对象执行加密和解密操作，同时保持对加密对象所用密钥的控制权。借助 SSE-C，您无需实施或使用客户端库来对 Amazon S3 中储存的对象执行加密和解密，但是需要对您发送到 Amazon S3 中执行对象加密和解密操作的密钥进行管理。当您希望维护自己的加密密钥而不想实施或使用客户端加密库时，请使用 SSE-C。

SSE-KMS 可让您使用 [AWS Key Management Service](https://aws.amazon.com/cn/kms/) (AWS KMS) 来管理您的加密密钥。使用 AWS KMS 管理您的密钥有几项额外的好处。利用 AWS KMS，会设置几个单独的主密钥使用权限，从而提供额外的控制层并防止 Amazon S3 中存储的对象受到未授权访问。AWS KMS 提供审查跟踪，因此您能看到谁使用了您的密钥在何时访问了哪些对象，还能查看用户在没有解密数据的权限下所作的访问数据失败尝试次数。同时，AWS KMS 还提供额外的安全控制，从而支持客户努力符合 PCI-DSS、HIPAA/HITECH 和 FedRAMP 行业要求。

使用 [Amazon S3 加密客户端](http://docs.amazonwebservices.com/AWSJavaSDK/latest/javadoc/com/amazonaws/services/s3/AmazonS3EncryptionClient.html)之 类的加密客户端库，您可以保持对密钥的控制并使用您选择的加密库完成对象客户端侧的加密和解密。一些客户倾向于对加密和解密对象拥有端到端的控制权；这样 一来，只有经过加密的对象才会通过互联网传输到 Amazon S3。如果您想掌握对加密密钥的控制权，应该使用客户端库，这样便可实施或使用客户端加密库，同时在将对象传输到 Amazon S3 进行储存之前需要对其进行加密。

### 问：Amazon S3 的持久性如何？

Amazon S3 Standard 和 Standard – IA 的设计可在指定年度内为对象提供 99.999999999% 的持久性。这种持久性级别对应的平均年对象损失率预计为 0.01%。例如，如果您使用 Amazon S3 存储 10,000 个数据元，则平均每 10,000,000 年发生一次数据元丢失。此外，Amazon S3 可以抵御在两个设施同时发生的数据丢失。

对于任何环境，最佳实践是做好备份，并准备好防范恶意或意外用户错误的措施。对于 S3 数据，最佳实践包括安全访问权限、跨区域复制、版本控制和经常测试的有效备份。

### 问：Amazon S3 的设计如何达到 99.999999999% 的持久性？

Amazon S3 Standard 和 Standard – IA 将您的对象冗余存储在分布于 Amazon S3 地区的多个设施的多台设备上。该服务可以快速检测和修复任何丢失冗余，从而抵御同时发生的设备故障。在处理对存储数据的请求时，该服务会在返回 SUCCESS 之前，将您的数据元冗余存储于多个设施。Amazon S3 还定期使用校验和来验证您的数据完整性。

### 问：什么是版本控制？

通过版本控制，您可以保留、提取和恢复存储在 Amazon S3 存储段中的每个数据元的每个版本。一旦您为存储段启用版本控制，Amazon S3 将在您每次执行 PUT、POST、COPY 或 DELETE 操作时保留现有数据元。默认情况下，GET 请求将提取最近写入的版本。可通过在请求中指定版本，提取已覆盖数据元或已删除数据元的旧版本。

### 问：如何确保我保留的版本得到最大保护？

版本控制的 MFA Delete 功能采用了[多重验证](http://aws.amazon.com/mfa/)， 可用于提供另一个安全层。默认情况下，对您的 Amazon S3 存储段的所有请求都需要您的 AWS 账户证书。如果您在 Amazon S3 存储段上利用 MFA Delete 功能启用了版本控制，则需要以下两种形式的身份验证才能永久删除数据元的某个版本：您的账户证书、来自您拥有的身份验证设备的有效六位代码和序列号。要了 解有关利用 MFA Delete 功能启用版本控制的更多信息，包括如何购买和激活身份验证设备，请参阅 [Amazon S3 技术文档](http://docs.amazonwebservices.com/AmazonS3/latest/dev/Versioning.html)。

### 问：什么是 S3 Standard – Infrequent Access？

Amazon S3 Standard – Infrequent Access (Standard – IA) 是 Amazon S3 存储类别，用于不频繁访问但在需要时也要求快速访问的数据。Standard – IA 提供较高的持久性、吞吐量和较低的 Amazon S3 Standard 延迟，并且每 GB 的存储价格和检索费用都较低。成本较低且性能出色使得 Standard – IA 成为长期存储和备份的理想选择，也非常适用于灾难恢复的数据存储。Standard – IA 存储类别被设置在对象级别，并可在相同的存储桶中作为 Standard 数据存在，从而让您可以使用生命周期政策在存储类别间自动转移对象，无需更改任何应用程序。

### 问：如何将我的数据导入 Standard – IA？

有两种方式可以将数据从 S3 导入 Standard – IA。通过在 x-amz-storage-class 标头中指定 STANDARD\_IA，您可以直接将数据放入 Standard – IA。您可以通过设置生命周期策略来将对象从 Standard 转移到 Standard – IA。

### 问：Standard – IA 是否有最低持续时间？

Standard – IA 的设计适用于长期但非频繁访问的数据（已保留了数月或数年）。30 天内从 Standard – IA 删除的数据将按照完整的 30 天收费。请查看 [Amazon S3 定价页面](https://aws.amazon.com/s3/pricing/)获取有关 Standard – IA 定价的信息。

### 问：Standard – IA 是否有最小对象大小？

Standard – IA 的设计适用于较大对象，最小对象大小为 128KB。小于 128KB 的对象将产生存储费用，并按 128KB 计费。比如，S3 Standard – IA 中 6KB 的对象将产生 6KB 的 S3 Standard – IA 存储费用，而剩下的最小对象大小（等于 122KB）将按照 S3 Standard – IA 存储费用收取。

### 问：可以免费恢复多少数据？

您每月最多可以免费恢复存储在 Amazon Glacier 中的 Amazon S3 数据的 5%。一般而言，这足以满足您备份和存档需要。每月 5% 的最高免费恢复限额是按日比例计量的。例如，您在某一天，将 12 TB 的 Amazon S3 数据归档到 Amazon Glacier，那么这一天您可以免费恢复 20.5 GB 数据（假定该月为 30 天，则为：12 TB x 5% / 30 天 = 20.5 GB）。

### 问：如何开启 CRR？

CRR 是存储桶级的配置。在不同区域中指定目标存储桶用于复制，这样就可以对来源存储桶开启 CRR 配置。还可以使用 AWS 管理控制台、REST API、AWS CLI 或 AWS 软件开发工具包来开启 CRR。要开启 CRR，必须对来源存储桶和目标存储桶都打开版本控制功能。

### 问：在 Transfer Acceleration 和 Amazon CloudFront 的 PUT/POST 之间，我应该如何选择？

Transfer Acceleration 优化了 TCP 协议，并在客户端与 S3 存储桶之间添加了更多智能，因此如果需要更高的吞吐量，Transfer Acceleration 就是更好的选择。如果您的对象小于 1GB，或者如果数据集小于 1GB，则应该考虑使用 Amazon CloudFront 的 PUT/POST 命令来优化性能。

### 问：在 Transfer Acceleration 和 AWS Snowball 之间，我应该如何选择？

要一次性移动大批量数据，AWS Import/Export Snowball 就是客户的理想选择。AWS Snowball 的周转时间通常为 5-7 天。一般来说，通过一条充分利用的 1Gbps 线路，Transfer Acceleration 在同样的时间内最多可以传输 75TB 数据。总之，如果通过 Internet 传输所需的时间超过一个星期，或者如果需要反复传输作业且可用带宽超过 25Mbps，Transfer Acceleration 就是不错的选择。另一个选择是同时使用两者：利用一个 AWS Snowball（或一系列 AWS Snowball）执行最初繁重的传输任务，然后利用 Transfer Acceleration 传输递增的日常变更。

### 问：我需要更新存储桶和 IAM 策略吗？

是的，如果您使用策略授予或限制通过 IP 地址的访问，则需要在切换至“双堆栈”终端节点之前更新这些策略以涵盖相关的 IPv6 范围。如果您的存储桶授予或限制对特定 IAM 用户的访问，您也需要在切换至“双堆栈”终端节点之前，让 IAM 策略管理员审核这些用户的 IAM 策略，以确保他们能够合理访问相关的 IPv6 范围。无法做到这些可能会导致客户端在开始使用 IPv6 时，错误失去或获得存储桶的访问权限。

### SNS

### 问：使用 Amazon SNS 有哪些好处？

Amazon SNS 在构建和集成松散耦合的分布式应用程序方面具备多种优势，这也使其成为一种多功能的选择：

* 基于推送的即时传送（无轮询）
* 简单的 API，与应用程序轻松集成
* 经由多种传输协议灵活传送消息
* 经济高效、按实际使用量付费的模式，无前期费用
* 基于 Web 的 AWS 管理控制台为用户提供了简便的点选式界面

### 问：Amazon SNS 的运行原理是什么？

动手使用 Amazon SNS 非常简单。开发人员必须首先创建一个“主题”（即一个“接入点”）– 标明特定的主题或事件类型，用来发布消息并允许客户端订阅通知。创建主题后，主题所有者可为其设置策略，例如，限制可以发布消息或订阅通知的人员，或者指 定支持哪些通知协议（即 HTTP/HTTPS、电子邮件、SMS）。订阅者是指有兴趣从关注的主题接收通知的客户端；它们可以订阅主题，也可以由主题所有者为其订阅。订阅者需要 为传送的通知指定协议和终端节点（URL、电子邮件地址、电话号码等）。当发布者有需要通知订阅者的信息或更新时，他们可以向该主题发布一条消息 – 这样将立即触发 Amazon SNS 向所有适用的订阅者发送该消息。

### 问：Amazon SNS 与 Amazon SQS 有何不同？

Amazon SQS 和 Amazon SNS 都是 AWS 中的消息发送服务，但为开发人员提供了不同的优势。Amazon SNS 允许应用程序通过“推送”机制向多个订阅者发送时间关键型消息，并且无需定期检查或“轮询”更新。Amazon SQS 是供分布式应用程序使用的消息队列服务，它通过轮询模式交换消息，可用于解耦收发组件。Amazon SQS 使分布式应用程序组件可以灵活地收发消息，并且不要求每个组件同时可用。

### 问：用户如何确保向我的主题发送的消息是安全的？

针对 Amazon SNS 的所有 API 调用都会根据该用户的 AWS ID 和签名进行验证。此外，我们建议用户通过连接到安全的 SSL 终端节点，确保网络传输数据的安全性。

### 问：是否可删除已发布的消息？

不可以，一旦将消息成功发布到主题，就无法再撤消。

### 问：我应该将哪些 SMS 消息标记为“事务型”？

您应该将有关业务优先事项的 SMS 消息标记为“事务型”。这可以确保含有一次性密码 (OTP) 或 PIN 的消息在具备最高交付可靠性的情况下通过路由发送。在美国以外的国家/地区，此类路由通常比“促销型”消息路由价格昂贵。您绝对不应将市场营销信息标记为 “事务型”，因为这会违反某些国家/地区的当地规制政策，否则，您的账户可能会被标记为滥用并暂停。

### 问：我应该将哪些 SMS 消息标记为“促销型”？

您应该将含有市场营销信息的 SMS 消息标记为“促销型”。Amazon SNS 可确保此类消息通过具有一定交付可靠性但成本却比最可靠的路由少很多的路由发送。这还可以让 Amazon SNS 根据当地法律法规的规定处理和发送您的消息。

### 问：我是否需要先向某个 SNS 主题订阅电话号码才能向其发送 SMS 消息？

现在，您无需先向某个 SNS 主题订阅电话号码就可以向其发送 SMS 消息。您可以直接使用 Amazon SNS 控制台或 Amazon SNS API 中的“Publish”申请向某个电话号码发布消息。

### 问：SMS 消息是否支持基于时间或按计划发送？

不支持。Amazon SNS 目前不支持基于时间或按计划发送。

### 问：我该如何追踪我的 SMS 消息的发送状态？

通过启用 Amazon SNS 中的“Delivery Status”功能，您可以获取有关各个消息的以下信息：Message ID、发送时间、目标电话号码、处置、处置原因（如果适用）、价格以及驻留时间。

### 问：什么是原始消息传输？

您现在可以选择让消息以原始形式传输，即和您发布时的消息形式完全一样。默认情况下，消息会以 JSON 编码进行传输，JSON 编码提供消息和主题的元数据。原始消息传输可以通过设置订阅的“RawMessageDelivery”属性来启用。该属性可以使用 AWS 管理控制台或者 API SetSubscriptionAttributes 来设置。

### 问：如果订阅的原始消息传输属性未设定，默认行为是什么？

如果该属性未设定，消息当前会默认以 JSON 形式传输。这确保了现有的应用程序会继续如期运行。

### 问：什么是直接寻址？如何工作？

直接寻址让您可以将通知直接提供给单一终端节点，而不是将相同的消息发送给一个主题的所有订阅者。如果您想将精准定位的消息发 送给每一名接收者，该功能便可派上用场。当您在 SNS 注册设备令牌时，SNS 便会创建与此令牌对应的终端节点。您可以像将内容发布到主题一样来将内容发布到令牌终端节点。您可以直接发布通知的文本，或利用平台特定功能（诸如更新应 用程序的徽章计数）的优势发布平台特定负载。直接寻址目前仅限推送通知终端节点。

### 问：SNS 是否支持 SMS 或电子邮件直接寻址？

否。此时，直接寻址将仅支持移动推送终端节点（APNS、GCM、ADM、WNS、MPNS 和百度）。

### 问：什么是存活时间 (TTL)？

可与 SNS 一起的某些消息仅在有限的时间段内相关或有价值。现在，使用 Amazon SNS，您可以为每条消息设定 TTL（存活时间）值。当指定消息超过 TTL 且未被用户提交或读取时，该消息即被删除。TTL 以秒为单位并与发布调用的时间相关。

### 问：TTL 消息属性是否覆盖在消息有效负载中指定的 TTL？

是。 Google GCM 和 Amazon ADM 支持您在消息净负荷内指定 TTL。 如果您在消息净负荷内指定一个 TTL，同时还在消息属性内指定一个 TTL，则 SNS 将遵循消息属性。

### 问：哪些 SNS 终端节点支持 TTL？

您可以通过以下移动推送终端节点使用 TTL：APNS、APNS\_Sandbox、GCM、ADM、百度和 WNS。 Microsoft MPNS 当前不支持 TTL。 TTL 也不支持用于 SQS、HTTP、电子邮件或 SMS 终端节点。

### 问：AWS Lambda 函数和 Amazon SNS 有何用？

通过将 AWS Lambda 函数订阅到 Amazon SNS 主题，您可以执行自定义消息处理。您可以调用 AWS Lambda 函数来提供自定义消息发送处理，方法是先将消息发布到一个 AWS Lambda 函数，再让 Lambda 函数修改一条消息（例如对语言进行本地化），最后对消息进行过滤并将其发送给其他主体和终端节点。已经发送 Amazon SNS 通知（例如 Amazon CloudWatch）的应用程序和服务现在可以立即利用 AWS Lambda 的优势，不需要调配或管理基础设施来进行自定义消息处理。您还可以使用发送到 AWS Lambda 函数功能来发布到其他 AWS 服务，例如 Amazon Kinesis 或 Amazon S3。您可以将 AWS Lambda 函数订阅到 Amazon SNS 主题，然后让 Lambda 函数轮流写入到另一项服务。

### 问：我的 AWS Lambda 函数需不需要与所使用的 Amazon SNS 处在相同的区域？

您可以将 AWS Lambda 函数订阅到任意区域中的 Amazon SNS 主题。

### 问：调用 AWS Lambda 函数会不会产生数据传输费用？

将消息发送到 AWS Lambda 函数会产生数据传输费用。更多信息请参考[定价](http://aws.amazon.com/sns/pricing/)。

### SQS

### 问：Amazon SQS 可以用来做什么？

由于 Amazon SQS 具有很高的可扩展性，而且您只需按实际用量付费，因此您可以从小规模开始，然后根据业务需要扩展应用程序，这样既不影响性能，也不影响可靠性。借助 Amazon SQS，您可以专注于构建稳健而复杂的基于消息的应用程序，不必再担心消息的存储和管理问题。

某些具体用途如下：

* 将 Amazon SQS 与其他 AWS 服务集成，让应用程序更加灵活、更加可靠。
* 使用 Amazon SQS 创建工作队列，其中每条消息都是一项等待处理的任务。让一台或多台计算机从消息对列中读取任务并处理任务。
* 构建微服务架构并使用消息队列来连接微服务。
* 将重要业务事件的通知保存在 Amazon SQS 消息队列中。每个事件在消息队列中均有一条对应的消息，需要知晓该事件的应用程序可以读取和处理对应的消息。

### 问：Amazon SQS 相对于自主或打包式消息队列系统有哪些优势？

与构建自己的软件来管理消息队列或使用前期需要花费大量的时间进行开发和配置的商用或开源消息队列系统相比，使用 Amazon SQS 具有若干优势。

其他方案需要持续进行硬件维护，并会占用系统管理资源。如果需要冗余消息存储以确保在出现硬件故障时不会丢失消息，那么这些系统的配置和管理将更为复杂。

相反，Amazon SQS 不需要管理开销，而且基本不需要配置。此外，Amazon SQS 可以大规模处理工作，每天处理数十亿条消息。您可以在不进行任何配置的情况下增加或减少向 Amazon SQS 发送的流量。此外，Amazon SQS 还可以实现极高的消息持久性，让您和您的利益相关者更加放心。

### 问：什么时候应该使用 Amazon Simple Workflow Service (Amazon SWF) 而不使用 Amazon SQS？

[Amazon SWF](https://aws.amazon.com/swf/) 和 [Amazon SQS](https://aws.amazon.com/sqs/) 都可以用来开发分离的分布式应用程序：

* Amazon SWF 用于开发高度可扩展的应用程序，并能实现可审核性。
* Amazon SQS 可以提供可靠并且高度可扩展的托管队列，用于发送和接收消息。

虽然可以使用 Amazon SQS 来构建用于协调分布式应用程序的基本工作流程，但这对于 Amazon SWF 而言是一项开箱即用的功能，并且 Amazon SWF 还能提供其他应用程序层面的功能。

我们建议您同时试用 Amazon SQS 和 Amazon SWF，以确定哪款解决方案最符合您的需求。

### 问：Amazon SQS 的费用是多少？

您只需按实际用量付费，而且没有最低费用。

在大多数区域，Amazon SQS 费用为每 100 万个请求 0.50 USD，再加上从 Amazon SQS 传出数据的数据传输费

### 问：是否可以将 Amazon SQS 与其他 AWS 服务结合使用？

可以。您可以将 Amazon SQS 与 Amazon EC2、Amazon EC2 Container Service (Amazon ECS) 和 AWS Lambda 等计算服务以及 Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 等存储和数据库服务结合使用，从而让应用程序具有更高的灵活性和可扩展性。

分离的分布式应用程序就是一种常见的使用案例。其中多个组件或模块需要互相通信，但不能同时处理相同数量的工作。在这种情况下，Amazon SQS 消息队列可以承载消息，供 Amazon EC2 实例上运行的应用程序进行处理。

Amazon EC2 实例可以读取消息队列、处理任务，然后将结果作为消息发布到另一 Amazon SQS 消息队列（可能由其他应用程序进行进一步处理）。由于 Amazon EC2 允许应用程序动态扩展和缩减，因此应用程序开发人员可以根据 SQS 队列中的消息量，使用 Auto Scaling 改变计算实例的数量，确保任务得以及时处理。

### 问：Amazon SQS 是否提供对消息的先入先出 (FIFO) 访问？

Amazon SQS 支持宽松的 FIFO 功能，会尽可能保持消息顺序。但是，由于我们为了让 Amazon SQS 可以大规模扩展而采用了分布式架构，因此我们无法保证您始终能够按照发送消息的先后顺序来接收消息 (FIFO)。

如果您的系统要求保持消息顺序，您可以在每条消息中添加排序信息，以便系统在接收消息时将其排序。

### 问：Amazon SQS 如何允许多个读取者访问同一消息队列，而不会丢失消息或重复处理消息？

每个 Amazon SQS 队列都具有可配置的可见性超时。当系统从队列中读取一条消息时，任何其他读取者在指定时间都看不到该消息。只要消息的处理时间短于可见性超时，则每条消息就都会得以处理并被删除。

如果处理消息的组件出现故障或不可用，那么可见性超时结束后，读取消息队列的任何组件就可以再次看到该消息。这可以让多个组件从同一消息队列中读取消息，并且每个组件负责处理不同的消息。

### 问：消息最长可见性超时时间是多少？

Amazon SQS 消息的最长可见性超时时间为 12 小时。

### 问：什么是 Amazon SQS 长轮询？

Amazon SQS 长轮询是从 Amazon SQS 队列中检索消息的一种方式。常规的短轮询会立即返回响应，即使轮询的消息队列为空；而长轮询只有在消息进入消息队列或长轮询超时时才返回响应。

如果要从 Amazon SQS 队列中检索暂时不可用的消息，那么长轮询是一种成本较低的方式。因为您可以减少接收空消息的次数，所以使用长轮询可以降低 SQS 的使用成本

### 问：如何将相同的消息群发到多个 Amazon SQS 队列？

1. 使用 Amazon SNS 创建一个主题。
2. 创建多个 Amazon SQS 消息队列并为其订阅该 Amazon SNS 主题。
3. 发送到 Amazon SNS 主题的所有消息都会被群发到 Amazon SQS 消息队列。

### 问：为什么会有单独的 ReceiveMessage 和 DeleteMessage 操作？

当 Amazon SQS 返回消息给您时，无论您实际上是否收到消息，该消息都会保存在消息队列中。您需要负责删除消息，而且发送删除请求即表明您已处理了该消息。

如果您不删除消息，则 Amazon SQS 会在收到另一个接收请求时传输该消息。

### 问：消息在 Amazon SQS 消息队列中可以保留多久？

较长消息的保留期可以实现更大的灵活性，让消息产生和消息使用之间的间隔时间更长。

您可以将 Amazon SQS 消息保留期配置为 1 分钟至 14 天之间的值。默认为 4 天。一旦达到消息保留期限，您的消息就会被自动删除。

### 问：如何配置 Amazon SQS 的最大消息大小？

要配置最大消息大小，请使用控制台或 SetQueueAttributes 方法来设置 MaximumMessageSize 属性。该属性用于指定 Amazon SQS 消息可以包含的字节数限值。可以将限值设为 1024 字节 (1KB) 到 262144 字节 (256KB) 之间的值。

### 问：如何标识我希望与之共享消息队列的另一个 AWS 用户？

Amazon SQS API 使用 AWS 账户来标识 AWS 用户。

### 问：Amazon SQS 是否支持匿名访问？

支持。您可以配置访问策略，允许匿名用户访问消息队列。

## Storage Gateway

### 问：AWS Storage Gateway 是什么？

AWS Storage Gateway 服务将内部软件设备与基于云的存储连接起来，在企业的内部 IT 环境和 AWS 的存储基础设施之间提供无缝、安全的集成。使用此服务，您可以安全地将数据存储到 AWS 云，以便享用可扩展且经济实惠的存储。AWS Storage Gateway 支持当前应用程序使用的行业标准存储协议。它通过本地维护经常访问的数据，并且在 Amazon Simple Storage Service (Amazon S3) 或 Amazon Glacier 上加密并存储所有数据来提供低延迟性能。

AWS Storage Gateway 支持三种配置：网关缓存卷、网关存储卷和网关虚拟磁带库 (VTL)。

*网关****缓存****卷：*您能以低成本且持久的方式将主要数据存储在 Amazon S3 中，并将您经常访问的数据保留在本地。网关缓存卷可显著节省用于主存储的成本，使您尽量避免扩展内部存储，同时还能对经常访问的数据进行低延迟访问。除了 使用网关缓存卷将主要数据存储在 Amazon S3 中，您还可以拍摄 Amazon S3 中的网关缓存卷数据的时间点快照，从而能够创建既节省了空间又控制了版本的卷副本，以满足数据保护和各种数据重复利用的需求。

*网关****存储****卷：*如果您需要快速访问整个数据集，则可以配置网关以便在本地存储主要数据，并将该数据的时间点快照异 步备份到 Amazon S3。网关存储卷可为您提供耐久且价格低廉的场外备份，例如，当您出于灾难恢复目的需要替代容量时，可以在本地或从 Amazon EC2 恢复这些备份。

*网关虚拟磁带库 (VTL)：*使用网关 VTL，您可以拥有无限的虚拟磁带集合。每个虚拟磁带都可以存储在采用 Amazon S3 的虚拟磁带库或采用 Amazon Glacier 的虚拟磁带架中。虚拟磁带库可提供一个符合行业标准的 iSCSI 接口，您的备份应用程序能够通过此接口在线访问虚拟磁带。如果您不再需要立即或经常访问虚拟磁带上的数据，则可使用备份应用程序将数据从其虚拟磁带库移到 虚拟磁带架中，以便进一步减少存储成本。

### 问：AWS Storage Gateway 的运行原理是什么？

AWS Storage Gateway 的软件设备可作为虚拟机 (VM) 映像下载，您可将该映像安装在数据中心的主机上。安装网关并通过激活过程将其与 AWS 账户关联后，您即可使用 AWS 管理控制台创建网关缓存卷、网关存储卷或网关-VTL 虚拟磁带库，它们可作为 iSCSI 设备供内部应用程序安装。

*网关缓存卷*允许您利用 Amazon S3 存储主要数据，同时将其中需经常访问的那部分数据保留在本地缓存中。这些卷可帮助您尽量避免扩展内部存储基础设施，同时让您的应用程序能低延迟地获取经常 访问的数据。您可以创建容量高达 32TB 的存储卷，并从本地应用程序服务器将其作为 iSCSI 设备安装。这些卷中写入的数据存储在 Amazon S3 中，而本地存储硬件上只存储近期写入和读取的数据的缓存。您还能以 Amazon EBS 快照的形式拍摄 Amazon S3 中的网关缓存卷数据的时间点快照，从而创建既节省了空间又控制了版本的卷副本，以满足数据保护和各种数据重复利用的需求。

*网关存储卷*在本地存储您的主要数据，同时将该数据异步备份到 AWS。这些卷在为您的本地应用程序提供耐久的场外备份的同时，也为本地应用程序提供对整个数据集的低延迟访问。 您可以创建容量高达 16TB 的存储卷，并从本地应用程序服务器将其作为 iSCSI 设备安装。网关存储卷中写入的数据存储在您的本地存储硬件，并以 Amazon EBS 快照的形式异步备份到 Amazon S3。

借助*网关虚拟磁带库 (VTL)*，您可以将物理磁带基础设施无缝更换为虚拟磁带基础设施。每个网关-VTL 都可为您的备份应用程序提供基于 iSCSI 的行业标准虚拟磁带库 (VTL)，它包括虚拟介质更换器和磁带驱动器。您可以使用 AWS 管理控制台在您的虚拟磁带库中创建虚拟磁带。每个虚拟磁带库可容纳多达 1500 个虚拟磁带，合计最大容量为 1PB。虚拟磁带由备份应用程序通过其标准的媒体库存程序进行搜索。虚拟磁带库中的虚拟磁带可立即访问，并由 Amazon S3 提供支持。您的备份应用程序可以通过使用虚拟介质更换器将虚拟磁带安装到虚拟磁带驱动器，对虚拟磁带中的数据执行读写操作。

为了以经济高效的方式对不需要经常访问的数据进行长期保留，您可以使用备份应用程序将虚拟磁带从一个或多个虚拟磁带库迁移到由 Amazon Glacier 支持的虚拟磁带架 (VTS) 中。在激活第一个网关 VTL 时会自动创建虚拟磁带架。需要经常访问的虚拟磁带应存储在虚拟磁带库中。而无需经常检索的数据则可以存档到虚拟磁带架中。虚拟磁带库中的虚拟磁带可即时访 问，但虚拟磁带架中的虚拟磁带必须先检索并载入虚拟磁带库，然后才可访问。您可以使用 AWS 管理控制台从虚拟磁带架中检索虚拟磁带。从虚拟磁带架中检索的虚拟磁带大约会在 24 小时后可供访问，并将自动载入虚拟磁带库。

### 问：AWS Storage Gateway 可执行哪种类型的数据缩减？

AWS Storage Gateway 可以压缩正在传输的数据和静态数据，从而降低数据传输量和存储费用。在 AWS Storage Gateway VM 和 AWS 之间传输的所有数据，以及存储在 AWS 中的所有数据，都将被压缩。此外，AWS Storage Gateway VM 仅上传已更改的数据，从而最大程度地降低了数据传输量。

### 问：卷的最大容量是多少？

每个*网关缓存卷*最多可以存储 32 TB 的数据。写入至卷的数据将在本地硬件上缓存并异步上传至 AWS，以便实现持久的存储。

每个*网关存储卷*最多可以存储 16 TB 的数据。写入至卷的数据将存储在本地硬件上并异步备份至 AWS，以便获得时间点快照。

对于网关缓存卷和网关存储卷，网关都会先压缩数据，然后再将其传输到 AWS 并存储其中。这可以降低数据传输量和存储费用。卷存储不会进行预配置，您将依据存储在卷上的数据量，而非所创建的卷大小支付费用。

### 问：每个网关可以管理多少卷数据？

每个*网关缓存型网关* 最多可支持 32 个卷，这些卷最多可存储 1PB 数据（32 个卷，每个卷的大小为 32TB）。

每个*网关存储型网关* 最多可支持 32 个卷，这些卷最多可存储 512TB 数据（32 个卷，每个卷的大小为 16TB）。

### 问：如何将快照还原成网关卷？

使用 AWS 管理控制台，您可以基于 Amazon S3 中存储的快照创建新的网关卷。然后您可以将此卷作为 iSCSI 设备安装到内部应用程序服务器。

由于网关存储卷将主要数据存储在本地，因此，基于快照创建新卷时，网关会将快照中包含的数据下载到本地硬件，在那里该数据会成为新卷的主要数据。

由于网关缓存卷将主要数据存储在 Amazon S3 中，因此，在基于快照创建新卷时，您的网关会将该快照的数据保留在 Amazon S3 中，后者将在那里成为新卷的主要数据。

### 问：如何访问虚拟磁带中的数据？

必须先将包含您的数据的虚拟磁带存储在虚拟磁带库中，然后才能对其进行访问。虚拟磁带库中的虚拟磁带可即时访问。如果包含您的 数据的虚拟磁带存储在虚拟磁带架中，您必须先从虚拟磁带架中检索虚拟磁带。您可以使用 AWS 管理控制台检索虚拟磁带。首先选择虚拟磁带，然后选择您希望载入虚拟磁带的虚拟磁带库。大约需要 24 个小时后，检索到的虚拟磁带才能在选择的虚拟磁带库中可用。当虚拟磁带在虚拟磁带库中可用后，您可以通过备份应用程序利用虚拟磁带还原数据。