**Amazon Elastic File System（EFS）**

Amazon Elastic File System (Amazon EFS) 可提供简单、可扩展、完全托管的弹性 NFS 文件系统，以与 AWS 云服务和本地资源配合使用。它可在不中断应用程序的情况下按需扩展到 PB 级，随着添加或删除文件自动扩展或缩减，无需预置和管理容量，可自适应增长。

Amazon EFS 提供两种存储类：标准存储类和不频繁访问存储类 (EFS IA)。EFS IA 提供针对每天未访问的文件进行了成本优化的性价比。只需在文件系统上启用 EFS 生命周期管理，根据您选择的生命周期策略，未被访问的文件将自动且透明地迁移到 EFS IA。EFS IA 存储类仅需每月 0.025 USD/GB\*。

虽然工作负载模式各不相同，但客户通常会发现 80％ 的文件很少被访问（适用于 EFS IA），而 20％ 的文件则被频繁使用（适用于 EFS 标准），因此有效存储成本低至每月 0.08 USD/GB\*。Amazon EFS 透明地为公共文件系统命名空间中的两个存储类文件提供服务。

Amazon EFS 旨在为数千个 Amazon EC2 实例提供大规模并行共享访问模式，可让您的应用程序在一致、低延迟的状态下实现高水平的总吞吐量和 IOPS。

Amazon EFS 非常适合支持从主目录到业务关键型应用程序在内的各种使用案例。客户可以使用 EFS 将现有企业应用程序直接迁移到 AWS 云。其他使用案例包括：大数据分析、Web 服务和内容管理、应用程序开发和测试、媒体和娱乐工作流程、数据库备份和容器存储。

Amazon EFS 是一种用于在多个可用区 (AZ) 中存储数据以提供高可用性和持久性的区域服务。Amazon EC2 实例可以跨 AZ、区域和 VPC 访问文件系统，而本地服务器可以使用 AWS Direct Connect 或 AWS VPN 访问。

**Amazon Elastic Block Store（EBS）**

易于使用、适用于任何规模的高性能数据块存储

Amazon Elastic Block Store (EBS) 是一种易于使用的高性能数据块存储服务，旨在与 Amazon Elastic Compute Cloud (EC2) 一起使用，适用于任何规模的吞吐量和事务密集型工作负载。Amazon EBS 上部署着各种各样的工作负载，例如关系数据库和非关系数据库、企业应用程序、容器化应用程序、大数据分析引擎、文件系统和媒体工作流。

您可以从六种不同的卷类型中进行选择，以取得最佳的价格和性能平衡。您可以为高性能数据库工作负载（如 SAP HANA）实现个位数毫秒延迟，或为大型顺序工作负载（如 Hadoop）实现每秒达 GB 的吞吐量。您可以在不中断关键应用程序的情况下更改卷类型、调整性能或增加卷大小，从而在需要时获得经济高效的存储。

EBS 卷专为任务关键型系统而设计，可在可用区 (AZ) 内进行复制，并可轻松扩展到数 PB 的数据。此外，您可以将 EBS 快照与自动生命周期策略配合使用，以备份 Amazon S3 中的卷，同时确保数据的地理保护和业务连续性。

**优势**

### **任意工作负载都能高效使用**

### **可用性高，持久性强**

### **经济高效**

### **易于使用**

### **近乎无限的规模**

### **安全**

Amazon Simple Queue Service（SQS）

适用于微服务、分布式系统和无服务器应用程序的完全托管的消息队列

Amazon Simple Queue Service (SQS) 是一种完全托管的消息队列服务，可让您分离和扩展微服务、分布式系统和无服务器应用程序。SQS 消除了与管理和运营消息型中间件相关的复杂性和开销，并使开发人员能够专注于重要工作。借助 SQS，您可以在软件组件之间发送、存储和接收任何规模的消息，而不会丢失消息，并且无需其他服务即可保持可用。使用 AWS 控制台、命令行界面或您选择的 SDK 和三个简单的命令，在几分钟内即可开始使用 SQS。

SQS 提供两种消息队列类型。标准队列提供最高吞吐量、最大努力排序和至少一次传送。SQS FIFO 队列旨在确保按照消息的发送顺序对消息进行严格一次处理。

## 优势

### **消除管理开销**

### **可靠传送消息**

### **保证敏感数据安全**

### **以经济高效的方式进行弹性扩展**

Amazon DynamoDB

适用于任何规模的快速灵活的 NoSQL 数据库服务

Amazon DynamoDB 是一个键/值和文档数据库，可以在任何规模的环境中提供个位数的毫秒级性能。它是一个完全托管、多区域、多活动的持久数据库，具有适用于 Internet 规模应用程序的内置安全性、备份和恢复以及内存中缓存。DynamoDB 每天可处理超过 10 万亿个请求，并可支持每秒超过 2000 万个请求的峰值。

许多全球发展最快的企业，如 Lyft、Airbnb 和 Redfin，以及 Samsung、Toyota 和 Capital One 等企业，都依靠 DynamoDB 的规模和性能来支持其关键任务工作负载。

数十万 AWS 客户选择 DynamoDB 作为键值和文档数据库，用于其移动、Web、游戏、广告技术、物联网以及其他需要任何规模的低延迟数据访问的应用程序。为您的应用程序创建一个新表，其他的交给 DynamoDB。

## 优势

### 规模性能

DynamoDB 通过在任意规模环境中提供一致的个位数毫秒响应时间，支持世界上一些最大规模的应用程序。您可以构建吞吐量和存储空间几乎无限的应用程序。

### 无需管理服务器

DynamoDB 是无服务器服务，无需预配置、修补或管理服务器，也不需要安装、维护或操作软件。DynamoDB 可自动纵向扩展和缩减表，以针对容量做出调整并保持性能。

### 企业级

DynamoDB 支持 ACID 事务，使您能够大规模构建业务关键型应用程序。DynamoDB 默认加密所有数据，并为您的所有表提供细粒度的身份和访问控制。您可以立即创建数百 TB 数据的完整备份，而不会对您的表性能产生影响，并且可以恢复到先前的 35 天内的任何时间点，而无需停机。您还可以将 Amazon DynamoDB 表数据导出到 Amazon S3 中的湖内数仓，以执行任意规模的分析。DynamoDB 还提供有服务级别协议，从而确保可用性。

Amazon Redshift

Amazon Redshift 是一种运行快速、完全托管的 PB 级数据仓库，让您可以通过简单而经济高效的方式使用现有商业智能工具来分析所有数据。您可以从小规模开始，无需做出预先承诺，并且能够以不到传统解决方案十分之一的成本扩展到 PB 级。客户通常进行 3 倍压缩，以显著降低成本。

特色和优势

Amazon Redshift 使用列存储技术提高 I/O 效率，同时跨多个节点并行运行查询，从而提供快速的查询性能。Amazon Redshift 提供了定制的 JDBC 和 ODBC 驱动程序，您可以从我们控制台的“连接客户端”选项卡中进行下载，从而使用各种熟悉的 SQL 客户端。您也可以使用标准的 PostgreSQL JDBC 和 ODBC 驱动程序。通过与 Amazon S3、Amazon DynamoDB、Amazon Elastic MapReduce、Amazon Kinesis 或任何支持 SSH 的主机集成，数据加载速度可随集群大小呈线性提升。

借助 Amazon Redshift 的数据仓库架构，您可以自动处理大部分常见管理任务，这些任务涉及云数据仓库的预置、配置和监控等方面。连续、递增且自动地备份到 Amazon S3。快速恢复；您可以在几分钟内开始查询，同时数据会在后台缓冲。只需单击几下就可以跨区域启用灾难恢复。

内置安全机制。您可以保护静态数据和传输中的数据，并使用 Amazon VPC 隔离集群。所有的 API 调用、连接尝试、查询以及集群变动都会被记录，并可审计。您可以使用 AWS CloudTrail 来审计 Amazon Redshift API 调用。

跨区域：只有redshift 和S3

Amazon Relational Database Service (RDS)

只需单击数下，即可在云中设置、运行和扩展关系数据库。

Amazon Relational Database Service (Amazon RDS) 让您能够在云中轻松设置、操作和扩展关系数据库。它在自动执行耗时的管理任务（如硬件预置、数据库设置、修补和备份）的同时，可提供经济实用的可调容量。这使您能够腾出时间专注于应用程序，为它们提供所需的快速性能、高可用性、安全性和兼容性。

Amazon RDS 在多种类型的数据库实例（针对内存、性能或 I/O 进行了优化的实例）上均可用，并提供六种常用的数据库引擎供您选择，包括 Amazon Aurora、PostgreSQL、MySQL、MariaDB、Oracle Database 和 SQL Server。您可以使用 AWS Database Migration Service 轻松将您现有的数据库迁移或复制到 Amazon RDS。

Amazon Virtual Private Cloud(VPC)

在 AWS 云中逻辑隔离的虚拟网络上构建。

Amazon Virtual Private Cloud (Amazon VPC) 是一个让您能够在自己定义的逻辑隔离的虚拟网络中启动 AWS 资源的服务。您可以完全掌控您的虚拟联网环境，包括选择自己的 IP 地址范围、创建子网以及配置路由表和网络网关。您可以将 IPv4 和 IPv6 都用于 Virtual Private Cloud 中的大多数资源，从而有助于确保安全、轻松地访问资源和应用程序。

作为 AWS 的基础服务之一，Amazon VPC 使得自定义 VPC 的网络配置变得容易。您可以为 Web 服务器创建一个能访问互联网的公有子网。您还可以将后端系统（如数据库或应用程序服务器）安置在无 Internet 访问的私有子网中。Amazon VPC 让您可以使用安全组和网络访问控制列表等多种安全层，帮助对各个子网中 Amazon EC2 实例的访问进行控制

Amazon CloudWatch

AWS 和本地的 AWS 资源和应用程序的可观测性

Amazon CloudWatch 是一种面向开发运营工程师、开发人员、站点可靠性工程师 (SRE) 和 IT 经理的监控和可观测性服务。CloudWatch 为您提供相关数据和切实见解，以监控应用程序、响应系统范围的性能变化、优化资源利用率，并在统一视图中查看运营状况。CloudWatch 以日志、指标和事件的形式收集监控和运营数据，让您能够在统一查看在 AWS 和本地服务器上运行的资源、应用程序和服务。您可以使用 CloudWatch 检测环境中的异常行为、设置警报、并排显示日志和指标、执行自动化操作、排查问题，以及发现可确保应用程序

正常运行的见解。

## 优势

### 跨应用程序和基础设施的单一平台上的可观测性

### 在 AWS 和本地收集指标的最简单方法

### 改善运营绩效和资源优化

### 获取运营可见性和见解

### 从日志中获取可作为行动依据的见解

没法监测内存

AWS CloudTrail

跟踪用户活动和 API 使用情况

AWS CloudTrail 是一项支持对您的 AWS 账户进行监管、合规性检查、操作审核和风险审核的服务。借助 CloudTrail，您可以记录日志、持续监控并保留与整个 AWS 基础设施中的操作相关的账户活动。CloudTrail 提供 AWS 账户活动的事件历史记录，这些活动包括通过 AWS 管理控制台、AWS 开发工具包、命令行工具和其他 AWS 服务执行的操作。此事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。 此外，您可以使用 CloudTrail 来检测 AWS 账户中的异常活动。这些功能可帮助您简化分析和问题排查

Amazon ElastiCache

(内存数据库)

与 Redis 或 Memcached 兼容的完全托管型内存中数据存储。支持实时应用程序，提供亚毫秒级延迟。

Amazon ElastiCache 可使您在云中无缝设置、运行和扩展常见的开源兼容内存中数据存储。通过从高吞吐量和低延迟的内存数据存储中检索数据，构建数据密集型应用程序或提升现有数据库的性能。Amazon ElastiCache 是缓存、会话存储、游戏、地理空间服务、实时分析和队列等实时使用案例的常见选择。

Amazon ElastiCache 为需要亚毫秒级响应时间的要求最高的应用程序提供完全托管型 Redis（在 Stack Overflow 2020 年开发人员调查中被开发人员票选为最受欢迎的数据库）和 Memcached。

Elastic Load Balancing(ELB)

分配网络流量以提高应用程序的可扩展性

Elastic Load Balancing 在多个目标（如 Amazon EC2 实例、容器、IP 地址、Lambda 函数和虚拟设备）之间，自动分配传入的应用程序流量。它可以在单个可用区内处理不断变化的应用程序流量负载，也可以跨多个可用区处理此类负载。Elastic Load Balancing 提供四种负载均衡器，它们均能实现高可用性、自动扩展和可靠的安全性，因此能让您的应用程序获得容错能力。

Application Load Balancer（ALB）

负载均衡器 充当客户端的单一接触点。客户端将请求发送到负载均衡器，负载均衡器再将它们发送到具体目标（例如 EC2 实例）。要配置您的负载均衡器，可以创建目标组，然后将目标注册到目标组。您还可以创建侦听器来检查来自客户端的连接请求，并创建侦听器规则以将来自客户端的请求路由到一个或多个目标组中的目标。

Amazon CloudFront

快速、高度安全且可编程的内容分发网络 (CDN)

Amazon CloudFront 是一项快速内容分发网络 (CDN) 服务，可以安全地以低延迟和高传输速度向全球客户分发数据、视频、应用程序和 API，全部都在开发人员友好的环境中完成。

CloudFront 提供最先进的安全功能，包括领域级加密和 HTTPS 支持，与AWS Shield、AWS Web 应用防火墙和 Route 53 无缝集成，以防止多种类型的攻击，包括网络和应用层 DDoS 攻击。这些服务共同驻留在全球范围内的边缘网络位置，并通过 AWS 网络主干网连接，为您的用户提供更安全、性能和可用的体验。

CloudFront 可以无缝使用任何 AWS 源，例如 Amazon S3、Amazon EC2, Elastic Load Balancing 或任何自定义 HTTP 源。您可以使用安全和可编程的边缘计算功能 AWS Lambda@Edge 通过 CloudFront 自定义内容交付。

源不可以用DB

Amazon Kinesis

实时轻松收集、处理和分析视频和数据流

Amazon Kinesis 可让您轻松收集、处理和分析实时流数据，以便您及时获得见解并对新信息快速做出响应。Amazon Kinesis 提供多种核心功能，可以经济高效地处理任意规模的流数据，同时具有很高的灵活性，让您可以选择最符合应用程序需求的工具。借助 Amazon Kinesis，您可以获取视频、音频、应用程序日志和网站点击流等实时数据，也可以获取用于机器学习、分析和其他应用程序的 IoT 遥测数据。借助 Amazon Kinesis，您可以即刻对收到的数据进行处理和分析并做出响应，无需等到收集完全部数据后才开始进行处理。

Amazon Glacier

云中的低成本存档存储

Amazon Glacier 是成本极低的存储服务，为数据存档和备份提供安全而持久的存储。为了降低成本，Amazon Glacier 专门针对不经常访问的数据以及可以接受数小时检索时间的数据进行了优化。利用 Amazon Glacier，客户可以可靠地存储大量或少量数据。

公司通常会为数据存档超额付费。首先，他们会被迫为其存档解决方案预先支付昂贵的费用（这并不包括持续产生的营运开支，如电力、设施、人员配置和维护成本）。其次，由于公司必须对其自身的容量需求进行预测，为了确保有足够的容量用于数据冗余和意外增长，难免会超额拨备配置。所有这些情况的组合就导致了存储容量未得到充分利用，还大大浪费了金钱。使用 Amazon Glacier，您只需按实际用量付费。Amazon Glacier 改变了数据存档和备份的上述情况，因为您无需预先支付任何费用，支付非常低的价格即可进行存储，并且可以根据需要扩展或缩减使用量，而 AWS 负责处理完成数据保留所需的所有运营繁重工作。您只需单击几下 AWS 管理控制台，就可以设置 Amazon Glacier，然后选择上传任何数量的数据。

Amazon Route 53

将最终用户路由到互联网应用程序的可靠且经济高效的方法

Amazon Route 53 是一种可用性高、可扩展性强的云域名系统 (DNS) Web 服务。它的目的是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 www.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。Amazon Route 53 也与 IPv6 完全兼容。

Amazon 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，还可以将用户路由到 AWS 外部的基础设施。您可以使用 Amazon Route 53 配置 DNS 运行状况检查以将流量路由到正常的终端节点，或者独立监控应用程序及其终端节点的运行状况。Amazon Route 53 Traffic Flow 让您可以通过多种路由类型（包括基于延迟的路由、Geo DNS、临近地理位置路由和加权轮询）轻松管理全球流量，所有的路由类型都可与 DNS 故障转移进行组合，以实现各种低延迟容错架构。利用 Amazon Route 53 Traffic Flow 简单的可视化编辑器，您可以轻松管理如何将终端用户路由到应用程序的终端节点，无论是在单个 AWS 区域还是在分布于全球的区域都可实现。Amazon Route 53 还提供域名注册功能，您可以购买和管理域名（例如 example.com），且 Amazon Route 53 将自动为您的域配置 DNS 设置。

AWS Elastic Beanstalk

简单易行，无限扩展

AWS Elastic Beanstalk 是一项易于使用的服务，用于在熟悉的服务器（例如 Apache 、Nginx、Passenger 和 IIS ）上部署和扩展使用 Java、.NET、PHP、Node.js、Python、Ruby、GO 和 Docker 开发的 Web 应用程序和服务。

您只需上传代码，Elastic Beanstalk 即可自动处理包括容量预配置、负载均衡、自动扩展和应用程序运行状况监控在内的部署工作。同时，您能够完全控制为应用程序提供支持的 AWS 资源，并可以随时访问底层资源。

Elastic Beanstalk 不额外收费 – 您只需为存储和运行应用程序所需的 AWS 资源付费。

Amazon Aurora

与 MySQL 和 PostgreSQL 兼容的关系数据库，专为云而打造。性能和可用性与商用数据库相当，成本只有其 1/10。

Amazon Aurora 是一种与 MySQL 和 PostgreSQL 兼容的关系数据库，专为云而打造，既具有传统企业数据库的性能和可用性，又具有开源数据库的简单性和成本效益。

Amazon Aurora 的速度最高可以达到标准 MySQL 数据库的五倍、标准 PostgreSQL 数据库的三倍。它可以实现商用数据库的安全性、可用性和可靠性，而成本只有商用数据库的 1/10。Amazon Aurora 由 Amazon Relational Database Service (RDS) 完全托管，RDS 可以自动执行各种耗时的管理任务，例如硬件预置以及数据库设置、修补和备份。

Amazon Aurora 采用一种有容错能力并且可以自我修复的分布式存储系统，这一系统可以把每个数据库实例扩展到最高 128TB。它具备高性能和高可用性，支持最多 15 个低延迟读取副本、时间点恢复、持续备份到 Amazon S3，还支持跨三个可用区 (AZ) 复制。

您可以访问 Amazon RDS 管理控制台，创建第一个 Aurora 数据库实例并开始迁移 MySQL 和 PostgreSQL 数据库。

AWS WAF – Web 应用程序防火墙

保护您的 Web 应用程序免遭常见 Web 漏洞的攻击

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的攻击，这些漏洞可能会影响可用性、损害安全性或消耗过多的资源。AWS WAF 允许您创建防范常见攻击模式（例如 SQL 注入或跨站点脚本）的安全规则，以及滤除您定义的特定流量模式的规则，从而让您可以控制流量到达您的应用程序的方式。您可以通过适用于 AWS WAF 的托管规则快速入门，这是由 AWS 或 AWS Marketplace 卖家托管的一套预配置规则。适用于 WAF 的托管规则可以解决 OWASP 十大安全风险等问题。这些规则会随新问题的出现定期更新。AWS WAF 包含功能全面的 API，借此您可以让安全规则的创建、部署和维护实现自动化。

使用 AWS WAF，您只需按使用量付费。定价基于您部署的规则数量和您的应用程序收到的 Web 请求数量。无需预先承诺。

您可以将 AWS WAF 作为 CDN 解决方案的一部分部署到 Amazon CloudFront 上，也可以将其部署到位于 Web 服务器或来源服务器（运行于 EC2 上）之前的 Application Load Balancer、适用于您的 REST API 的 Amazon API Gateway 或者是适用于您的 GraphQL API 的 AWS AppSync 上。

AWS Shield

托管式 DDoS 防护

AWS Shield 是一种托管式分布式拒绝服务 (DDoS) 防护服务，可以保护在 AWS 上运行的应用程序。AWS Shield 提供持续检测和自动内联缓解功能，能够尽可能缩短应用程序的停机时间和延迟，因此您不需要联系 AWS Support 来获得 DDoS 防护。AWS Shield 有两个层级，分别为 Standard 和 Advanced。

所有 AWS 客户都可以使用 AWS Shield Standard 的自动防护功能，不需要额外支付费用。AWS Shield Standard 可以防护大多数以网站或应用程序为攻击对象并且频繁出现的网络和传输层 DDoS 攻击。将 AWS Shield Standard 与 Amazon CloudFront 和 Amazon Route 53 一起使用时，您将获得针对所有已知基础设施（第 3 层和第 4 层）攻击的全面可用性保护。

对于以在 Amazon Elastic Compute Cloud (EC2)、Elastic Load Balancing (ELB)、Amazon CloudFront、AWS Global Accelerator 和 Amazon Route 53 资源上运行的应用程序为目标的攻击，如果想要获得更高级别的防护，您可以使用 AWS Shield Advanced。除了 Standard 版本提供的常见网络和传输层防护之外，AWS Shield Advanced 还可以针对复杂的大型 DDoS 攻击提供额外的检测和缓解服务，让您能够近实时查看各种攻击，并且集成了 AWS WAF 这一 Web 应用程序防火墙。使用 AWS Shield Advanced，您还可以联系随时待命的 AWS DDoS 响应团队 (DRT) 并可以获得针对您 Amazon Elastic Compute Cloud (EC2)、Elastic Load Balancing (ELB)、Amazon CloudFront、AWS Global Accelerator 和 Amazon Route 53 费用中出现的 DDoS 相关高峰的全天候防护。

目前，客户可在全球所有 Amazon CloudFront、AWS Global Accelerator 和 Amazon Route 53 边缘站点使用 AWS Shield Advanced。通过为您的应用程序部署 Amazon CloudFront，您可以保护在全球任意位置托管的 Web 应用程序的安全。您的源服务器可以是 Amazon S3、Amazon Elastic Compute Cloud (EC2)、Elastic Load Balancing (ELB) 或 AWS 外部的自定义服务器。您还可以在以下 AWS 区域直接在弹性 IP 或 Elastic Load Balancing (ELB) 上启用 AWS Shield Advanced：弗吉尼亚北部、俄亥俄、俄勒冈、加利福尼亚北部、蒙特利尔、圣保罗、爱尔兰、法兰克福、伦敦、巴黎、斯德哥尔摩、新加坡、东京、悉尼、首尔和孟买。

为 传统负载均衡器 配置运行状况检查

您的 传统负载均衡器 会定期向其注册实例发送请求以测试其状态。这些测试称为运行状况检查。在执行运行状况检查时，运行状况良好的实例的状态为 InService。在执行运行状况检查时，运行状况不佳的任何实例的状态为 OutOfService。负载均衡器会对所有已注册实例执行运行状况检查，无论实例处于运行状况良好状态还是不佳状态。

负载均衡器仅将请求路由到正常的实例。当负载均衡器确定某个实例不正常时，会停止将请求路由到该实例。当实例恢复正常状态时，负载均衡器将恢复向该实例路由请求。

负载均衡器使用 Elastic Load Balancing 提供的默认运行状况检查配置或您配置的运行状况检查配置来检查已注册实例的运行状况。

如果您已将 Auto Scaling 组与 传统负载均衡器 关联，则可以使用负载均衡器运行状况检查确定 Auto Scaling 组中实例的运行状况。默认情况下，Auto Scaling 组会定期确定每个实例的运行状况。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的向 Auto Scaling 组添加 Elastic Load Balancing 运行状况检查。

Amazon Elastic Container Service

运行容器的高度安全、可靠且可扩展的方式

Amazon Elastic Container Service (Amazon ECS) 是一种完全托管的容器编排服务。出于其安全性、可靠性和可扩展性，Duolingo、Samsung、GE 和 Cookpad 等客户都使用 ECS 运行他们最敏感的任务关键型应用程序。

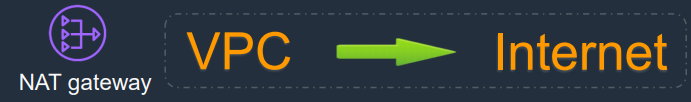
出于以下几个原因，ECS 是运行容器的最佳选择。首先，您可以选择使用 AWS Fargate 运行您的 ECS 集群，前者是容器的无服务器计算服务。使用 Fargate，您无需预置和管理服务器，而且可以为每个应用程序指定资源并为其付费，并通过设计隔离应用程序来提高安全性。其次，ECS 在 Amazon 内广泛用于支持 Amazon SageMaker、AWS Batch、Amazon Lex 等服务及 Amazon.com 的推荐引擎，从而确保对 ECS 进行广泛的安全性、可靠性和可用性测试。

此外，由于 ECS 是 Amazon 关键服务的基础支柱，它可以与 Amazon Route 53、Secrets Manager、AWS Identity and Access Management (IAM) 和 Amazon CloudWatch 等其他服务进行本机集成，为您提供部署和扩展容器的熟悉体验。ECS 还能够与其他 AWS 服务快速集成，从而为 ECS 带来新功能。例如，ECS 可使您的应用程序通过 Spot 和按需定价选项灵活使用 Amazon EC2 和AWS Fargate 组合。ECS 还与 AWS App Mesh 集成，后者是一个服务网格，可为您的应用程序带来丰富的可观察性、流量控制和安全功能。ECS 自推出以来发展迅速，目前每小时启动的容器数是 EC2 启动实例数的 5 倍。

Internet 网关的路由表



NAT 设备的路由表(ip4)



虚拟专用网关的路由表



VPC 对等连接的路由表



Classic Link 路由表（已过时）



VPC 终端节点的路由表



仅出口Internet网关的路由表(ip6)



中转网关的路由表



AWS CodeDeploy

实现代码部署自动化以确保应用程序的正常运行时间

AWS CodeDeploy 是一项将软件自动部署到各种计算服务（例如 Amazon EC2、AWS Fargate、AWS Lambda 和本地服务器）的完全托管的部署服务。借助 AWS CodeDeploy，您可以更轻松地快速发布新功能，避免在应用程序部署过程中出现停机，并简化应用程序的更新工作。您可以使用 AWS CodeDeploy 自动执行软件部署，而无需执行容易出错的手动操作。服务根据您的部署需求进行扩展。

# 优势

### 自动部署

### 最大程度地减少停机时间

### 集中控制

### 易于采用

AWS Security Token Service

AWS Security Token Service (AWS STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users). This guide describes the AWS STS API. For more information, see Temporary Security Credentials in the IAM User Guide.

For information about setting up signatures and authorization through the API, see Signing AWS API Requests in the Amazon Web Services General Reference. For general information about the Query API, see Making Query Requests in the IAM User Guide. For information about using security tokens with other AWS products, see AWS Services That Work with IAM in the IAM User Guide.

AWS安全令牌服务(AWS STS)是一种web服务，允许您为AWS身份和访问管理(IAM)用户或您所认证的用户(联邦用户)请求临时的、有限制权限的凭据。

本指南描述了AWS STS API。

更多信息，请参见IAM用户指南中的临时安全凭据。

有关通过API设置签名和授权的信息，请参见《Amazon Web服务通用参考》中的“签署AWS API请求”。

查询API的一般信息请参见《IAM用户指南》中的“请求查询”。

有关在其他AWS产品中使用安全令牌的信息，请参阅IAM用户指南中的“与IAM一起工作的AWS服务”。

Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) 是适用于 Amazon DynamoDB 的完全托管且高度可用的内存中的缓存，可实现高达 10 倍的性能提升（从数毫秒缩短到数微秒），即使在每秒处理的请求数量达到数百万个的情况下也是如此。

DAX 负责完成为 DynamoDB 表进行内存中的加速所需的所有繁重任务，使开发人员无需管理缓存失效、数据填充或集群管理。

现在，您可以集中精力为您的客户构建出色的应用程序，而无需担心规模性能。您不需要修改应用程序逻辑，因为 DAX 可与现有的 DynamoDB API 调用兼容。请参阅《DynamoDB 开发人员指南》，了解更多信息。

您只需在 AWS 管理控制台中单击几下，或使用 AWS 软件开发工具包即可启用 DAX。与 DynamoDB 一样，您只需为您实际预置的容量付费。访问定价页面，详细了解 DAX 定价。

AWS Storage Gateway

对几乎无限的云存储的本地访问权限

AWS Storage Gateway 是一项混合云存储服务，可让您从本地访问几乎不受限制的云存储。客户使用 Storage Gateway 简化存储管理，降低关键混合云存储用例的成本。其中包括将备份和存档移动到云、使用云存储支持的本地文件共享，以及为本地应用程序提供对 AWS 中数据的低延迟访问。

为了支持这些用例，Storage Gateway 提供了三种不同类型的网关：文件网关、磁带网关和卷网关，这些网关将本地应用程序无缝连接到云存储，从而在本地缓冲数据以进行低延迟访问。您的应用程序可以使用 NFS、SMB、iSCSI 等标准存储协议通过虚拟机或网关硬件设备连接到该服务。网关会连接到 Amazon S3、Amazon S3 Glacier、Amazon S3 Glacier Deep Archive、Amazon EBS 和 AWS Backup 等 AWS 存储服务，这些服务为 AWS 中的文件、卷、快照和虚拟磁带提供存储。该服务包括一种高度优化且高效的数据传输机制，拥有带宽管理、自动网络恢复能力。

Amazon FSx

Launch and run feature-rich and highly-performant file systems with just a few clicks

Amazon FSx makes it easy and cost effective to launch and run popular file systems that are fully managed by AWS. With Amazon FSx, you can leverage the rich feature sets and fast performance of widely-used open source and commercially-licensed file systems, while avoiding time-consuming administrative tasks such as hardware provisioning, software configuration, patching, and backups. It provides cost-efficient capacity with high levels of reliability, and integrates with a broad portfolio of AWS services to enable faster innovation.

Amazon FSx provides two file systems to choose from: Amazon FSx for Windows File Server for business applications and Amazon FSx for Lustre for compute-intensive workloads.

只需点击几下，就可以启动并运行功能丰富和高性能的文件系统

Amazon FSx使启动和运行完全由AWS管理的流行文件系统变得简单和经济。

使用Amazon FSx，您可以利用广泛使用的开源和商业许可文件系统的丰富特性集和快速性能，同时避免耗时的管理任务，如硬件配置、软件配置、补丁和备份。

它提供具有高可靠性的成本效益的容量，并与广泛的AWS服务组合集成，以实现更快的创新。

Amazon FSx提供了两个文件系统供您选择:用于业务应用程序的Windows文件服务器的Amazon FSx和用于计算密集型工作负载的Lustre的Amazon FSx。

# **Amazon 资源名称 (ARN)**

Amazon 资源名称 (ARN) 唯一标识 AWS 资源。当您需要在 AWS 全局环境中（比如 IAM 策略、Amazon Relational Database Service (Amazon RDS) 标签和 API 调用中）明确指定一项资源时，我们要求使用 ARN。

宣布推出 S3 智能分层 –

一种新的 Amazon S3 存储类

发布于: Nov 25, 2018

S3 智能分层是一种新的 Amazon S3 存储类，专为希望在数据访问模式发生变化时自动优化存储成本而不会影响性能或运营开销的客户而设计。S3 智能分层是第一个云对象存储类，通过在访问模式发生变化时在两个访问层（频繁访问层和不频繁访问层）之间移动数据来实现自动节省成本，非常适用于访问模式未知或不断变化的数据。

S3 智能分层将对象存储在两个访问层中：一个是针对频繁访问进行了优化的层，另一个是针对不频繁访问进行了优化的更低成本的层。每个对象每月只需支付少量的监控和自动化费用，S3 智能分层即可监控访问模式并将连续 30 天未访问的对象移动到不频繁访问层。S3 智能分层没有检索费用。如果日后访问了不频繁访问层中的对象，S3 智能分层会自动将其移回频繁访问层。在 S3 智能分层存储类中的访问层之间移动对象时，不会产生额外的分层费用。S3 智能分层旨在提供 99.9% 的可用性和 99.999999999% 的持久性，并提供与 S3 标准存储相同的低延迟和高吞吐量性能。

Amazon S3 功能包括 S3 对象标记、S3 跨区域复制和 S3 Select，所有这些功能都可与 S3 智能分层配合使用。客户可以通过 S3 API、CLI 和管理控制台开始使用 S3 智能分层，方法是将对象直接放入 S3 智能分层中或使用 S3 生命周期策略将对象从 S3 标准存储或 S3 标准-IA 存储移动到 S3 智能分层存储中。客户还可以将设置了 S3 生命周期策略的对象从 S3 智能分层存档到 Amazon S3 Glacier。

S3 智能分层现已在所有商业 AWS 区域和 AWS GovCloud（美国）提供。要了解有关 S3 智能分层的更多信息，请访问 Amazon S3 存储类页面。有关本次发布的更多信息，请阅读标题为“新增存储类 – 通过智能分层自动优化 Amazon S3 的成本”的 AWS 博客 »

AWS PrivateLink

在 VPC 与托管在 AWS 或本地的服务之间建立私有连接，而无需将数据暴露于互联网

AWS PrivateLink 可以在 VPC 与托管在 AWS 或本地的服务之间通过 Amazon 网络安全地提供私有连接。通过提供用于访问您的服务的私有终端节点，AWS PrivateLink 可确保您的流量不会暴露于公共互联网。AWS PrivateLink 让您可以在不同账户和不同 VPC 之间轻松连接各种服务，大幅简化网络架构。

AWS Database Migration Service

以最短的停机时间将您的数据库迁移至 AWS

已有超过 350000 个数据库使用 AWS Database Migration Service 完成迁移

AWS Database Migration Service 可帮助您快速并安全地将数据库迁移至 AWS。源数据库在迁移过程中可继续正常运行，从而最大程度地减少依赖该数据库的应用程序的停机时间。AWS Database Migration Service 可以在广泛使用的开源商业数据库之间迁移您的数据。

AWS Database Migration Service 支持同构迁移（例如从 Oracle 迁移至 Oracle），以及不同数据库平台之间的异构迁移（例如从 Oracle 或 Microsoft SQL Server 迁移至 Amazon Aurora）。借助 AWS Database Migration Service，您可以持续地以高可用性复制数据，并通过将数据流式传输到 Amazon Redshift 和 Amazon S3，将数据库整合到 PB 级的数据仓库中。了解更多有关受支持的源和目标数据库的信息。

如果数据库迁移的目标为 Amazon Aurora、Amazon Redshift、Amazon DynamoDB 或 Amazon DocumentDB（兼容 MongoDB），您可以免费使用 DMS 六个月。

AWS Secrets Manager

在整个生命周期中，轻松轮换、管理和检索数据库凭证、API 密钥和其他私密信息

AWS Secrets Manager 可帮助您保护访问应用程序、服务和 IT 资源所需的密钥。该服务使您能够轻松地跨整个生命周期轮换、管理和检索数据库凭证、API 密钥和其他密钥。用户和应用程序通过调用 Secrets Manager API 来检索密钥，无需对纯文本的敏感信息进行硬编码。Secrets Manager 通过适用于 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 的内置集成实现密钥轮换。此外，该服务还可以扩展到其他类型的密钥，包括 API 密钥和 OAuth 令牌。此外，Secrets Manager 使您能够使用精细权限来访问机密信息，并集中审核对 AWS 云、第三方服务和本地资源的密钥轮换。

## 优势

### 安全轮换私密信息

### 采用细粒度策略管理访问权限

### 集中保护和审计私密信息

### 按需付费

AWS Key Management Service (KMS)

轻松创建和控制用于对数据进行加密或数字签名的密钥

AWS Key Management Service (KMS) 可让您轻松创建和管理加密密钥，并控制其在各种 AWS 服务和应用程序中的使用。AWS KMS 是一种安全且有弹性的服务，它使用已经过 FIPS 140-2 验证或正在验证的硬件安全模块来保护您的密钥。AWS KMS 还能与 AWS CloudTrail 集成，从而为您提供所有密钥的使用记录，帮助您满足监管和合规性要求。

优势

完全托管

您可以通过定义在 AWS KMS 强制执行权限并处理密钥的持久性和物理安全性时密钥的使用权限来控制对加密数据的访问。

集中式密钥管理

AWS KMS 提供了单一控制点，用于管理密钥并在集成的 AWS 服务和您自己的应用程序之间以一致的方式定义策略。您可以从 AWS 管理控制台或使用 AWS SDK 或 CLI 轻松创建、导入、轮换、删除和管理密钥权限。

管理 AWS 服务的加密

AWS KMS 与 AWS 服务集成，可简化密钥使用以加密 AWS 工作负载中的数据。您可以选择所需的访问控制级别，包括在账户和服务之间共享加密资源的能力。KMS 会将密钥的所有使用记录到 AWS CloudTrail，以便为您提供访问加密数据的用户的独立视图，包括代表您使用这些数据的 AWS 服务。

在应用程序中加密数据

AWS KMS 与 AWS Encryption SDK 集成，使您可以使用受 KMS 保护的数据加密密钥在应用程序中进行本地加密。使用简单的 API，您还可以在自己的应用程序中构建加密和密钥管理，无论应用程序在何处运行。

对数据进行数字签名

AWS KMS 使您能够使用非对称密钥对执行数字签名操作，以确保数据的完整性。经过数字签名的数据的接收者可以验证签名是否具有 AWS 账户。

成本低廉

使用 AWS KMS 没有承诺用量也没有预付费用。您只需每月支付 1 美元即可存储您创建的任何密钥。AWS 服务为您创建的 AWS 托管密钥可以免费存储。使用或管理超出免费套餐的密钥时，将按要求付费。

安全

AWS KMS 使用已经过 FIPS 140-2 验证或正在验证的硬件安全模块 (HSM) 来生成密钥并对其进行保护。您的密钥仅可在这些设备中使用，并且永远不会将其保留为未加密状态。KMS 密钥从不会在创建其所在的 AWS 区域之外共享。

合规性

AWS KMS 的安全和质量控制已通过多种合规性计划认证，以简化您自己的合规性义务。AWS KMS提供了将密钥存储在您控制的 AWS CloudHSM 实例中的单租户 HSM 中的选项。

内置审计

AWS KMS 与 AWS CloudTrail 集成，可记录所有 API 请求，包括密钥管理操作和密钥使用情况。记录 API 请求可帮助您管理风险，满足合规性要求并进行取证分析。

Amazon Guard​Duty

提供智能威胁检测和持续监控，保护您的 AWS 账户、工作负载和数据

Amazon GuardDuty 是一种威胁检测服务，可持续监控恶意活动和未经授权的行为，从而保护您的 AWS 账户、工作负载和在 Amazon S3 中存储的数据。迁移到云后，账户和网络活动的收集与聚合变得异常简单，但安全团队对事件日志数据进行持续的分析以发现潜在的威胁，则可能十分耗时。GuardDuty 为您提供了经济高效的智能选项，从而持续检测在 AWS 中发生的威胁。此服务使用机器学习、异常检测和集成威胁情报等手段，识别潜在的威胁并确定优先级别。GuardDuty 对来自多个 AWS 数据源（例如 AWS CloudTrail 事件日志、Amazon VPC 流日志和 DNS 日志）的数百亿事件进行分析。只需在 AWS 管理控制台中几次点击，就可以启用 GuardDuty，无需部署或维护任何软件或硬件。GuardDuty 警报与 Amazon CloudWatch Events 集成，具有极好的可行动性，非常便于跨多个账户聚合，并且可以直接推送到现有的事件管理和工作流程系统。

Amazon EventBridge

无服务器事件总线，用于连接来自您自己的应用程序、SaaS 和 AWS 服务的应用程序数据

Amazon EventBridge 是一种无服务器事件总线，支持您使用自己的应用程序、集成软件即服务 (SaaS) 应用程序和 AWS 服务的数据轻松将应用程序连接到一起。EventBridge 提供来自事件源（例如 Zendesk、Datadog 或 Pagerduty）的实时数据流，并将该数据路由到 AWS Lambda 之类的目标。您可以设置路由规则来确定发送数据的目的地，以便构建能够实时响应所有数据源的应用程序架构。

EventBridge 让事件驱动型应用程序的构建变得简单，因为它可以为您完成事件摄取和传送、安全保障、授权以及错误处理工作。由于应用程序中的事件之间的联系日益紧密，您需要花费更多的精力来查找事件并了解其结构，才能编写出代码来响应这些事件。Amazon EventBridge Schema 注册表可将事件结构（即 Schema）存储在共享的中央位置，并将这些 Schema 映射至 Java、Python 和 Typescript 代码，从而让您能够在代码中以对象形式轻松使用事件。您可以从 AWS 管理控制台、API 或者适用于 Jetbrains（Intellij、PyCharm、Webstorm、Rider）和 VS 代码的软件开发工具包连接至 Schema 注册表并与之交互。

S3 Transfer Acceleration

Faster long-distance S3 uploads & downloads

Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet. S3 Transfer Acceleration (S3TA) reduces the variability in Internet routing, congestion and speeds that can affect transfers, and logically shortens the distance to S3 for remote applications. S3TA improves transfer performance by routing traffic through Amazon CloudFront’s globally distributed Edge Locations and over AWS backbone networks, and by using network protocol optimizations. You can turn on S3TA with a few clicks in the S3 console, and test its benefits from your location with a speed comparison tool. With S3TA, you pay only for transfers that are accelerated.

更快的远程S3上传和下载

对于大型对象的远程传输，Amazon S3传输加速可以使与Amazon S3之间的内容传输速度提高50-500%。

拥有拥有广泛用户的web或移动应用程序的客户，或者拥有远离S3存储区的应用程序的客户，可以在Internet上体验到长且可变的上传和下载速度。

S3传输加速(S3TA)减少了可能影响传输的Internet路由、拥塞和速度方面的可变性，并从逻辑上缩短了远程应用程序与S3的距离。

S3TA通过通过Amazon CloudFront全球分布的边缘位置和AWS骨干网路由流量，并通过使用网络协议优化，提高了传输性能。

只需在S3控制台中单击几下，就可以打开S3TA，然后使用速度比较工具从您的位置测试它的优点。

使用S3TA，您只需要为加速转账支付。

Lambda@Edge

在靠近用户的地方运行代码

Lambda@Edge 是 Amazon CloudFront 的一个功能，它可让您在靠近应用程序用户的地方运行代码，从而提高性能，降低延迟。使用 Lambda@Edge，您无需在全球多个地方预置或管理基础设施。您只需按使用的计算时间付费 — 代码未运行时不产生费用。

使用 Lambda@Edge，您可以将 Web 应用程序分布在全球并提高它们的性能（并且无需管理任何服务器），从而丰富您的 Web 应用程序。Lambda@Edge 根据 Amazon CloudFront 内容分发网络 (CDN) 生成的事件运行代码。您只需将代码上传到 AWS Lambda，后者将在靠近最终用户的 AWS 站点完成运行和扩展代码所需的一切操作，从而实现高可用性。