Amazon S3 提供了多种功能，可供您以各种方式组织和管理数据，从而支持特定使用案例、实现成本效率、实施安全性并满足合规要求。数据以对象的形式存储在名为“存储桶”的资源中，单个对象大小的上限为 5 TB。S3 的特性中还包括诸多功能，可以将元数据标签附加到对象，跨 S3 存储类移动和存储数据，配置并实施数据访问控制，防止未经授权的用户访问数据，运行大数据分析，以及在对象级别和存储桶级别监控数据。您可以通过 S3 访问点或直接通过存储桶主机名访问对象。

存储管理和监控

Amazon S3 具备平面的未分层结构并有多种管理功能，帮助各种规模和行业的客户按照能够为其业务和团队带来最大价值的方式组织数据。所有对象存储在 S3 存储桶中，可以按称为“前缀”的共享名称来组织。对于每个对象，您可以附加最多 10 个称为 S3 对象标签的键值对，这些键值对在对象的整个生命周期中可以创建、更新和删除。要跟踪对象及其对应的标签和前缀，您可以使用 S3 清单报告，其中列出了 S3 存储桶中的已存储对象或具有特定前缀的已存储对象，及其相应的元数据和加密状态。S3 清单可以配置为每天或每周生成报告。

存储管理

借助 S3 存储桶名称、前缀、对象标签和 S3 清单，您可以通过广泛的方式来分类和报告您的数据，然后配置其他 S3 功能以采取操作。 S3 批量操作使您无论存储成千上万还是数十亿个对象都变得非常简单，可在 Amazon S3 中管理任意规模的数据。使用 S3 批量操作，只需一个 S3 API 请求或者在 Amazon S3 管理控制台中的几次单击，您就可在存储桶之间复制对象，替换对象标签集，修改访问控制，以及从 Amazon S3 Glacier 恢复存档的对象。您还可以使用 S3 批量操作在对象上运行 AWS Lambda 函数，用于执行自定义的业务逻辑，例如处理数据或者转码图像文件。要开始使用，请使用 S3 清单报告指定目标对象列表或者提供自定义列表，然后从预填充的菜单中选择所需操作。S3 批量操作请求完成后，您会收到通知以及有关全部更改的完成报告。通过观看视频教程了解更多有关 S3 批量操作的信息。

Amazon S3 还支持帮助维护数据版本控制、防止意外删除以及在相同或不同的 AWS 区域中复制数据的功能。借助 S3 版本控制，您可以轻松地保存、检索和还原存储到 Amazon S3 存储桶中的某个对象的每个版本；这让您可以从意外的用户操作和应用程序故障中进行恢复。要防止意外删除，请在 S3 存储桶上启用多重验证 (MFA) 删除。如果您在启用了 MFA 删除的存储桶中尝试删除某个对象，存储桶会要求提供两种形式的身份验证：您的 AWS 账户凭证以及有效序列号、空格和显示在已批准身份验证设备（例如，硬件密钥卡或 Universal 2nd Factor (U2F) 安全密钥）上的六位代码的组合。

利用 S3 复制，您可将对象（及其对应的元数据和对象标签）复制到相同或不同的 AWS 区域，以减少延迟、确保合规性、安全性、灾难恢复和其他使用案例。S3 跨区域复制 (CRR) 配置到一个源 S3 存储桶，并将对象复制到位于其他 AWS 区域中的目标存储桶。 Amazon S3 同区域复制 (SRR) 在同一区域内的存储桶之间复制对象。Amazon S3 复制时间控制 (S3 RTC) 通过提供 SLA 和对复制时间的可见性来帮助您满足数据复制的合规性要求。

您还可以通过 S3 对象锁定实施一次写入，多次读取 (WORM) 策略。此 S3 管理功能在客户定义的保留期内阻止删除对象版本，让您能够通过实施保留策略来进一步保护数据或满足合规性要求。您可将工作负载从现有 WORM 系统迁移到 Amazon S3，并在对象级别或存储桶级别配置 S3 对象锁定，防止在预定义的保留到期日期或法律保留日期之前删除对象版本。具有 S3 对象锁定的对象会保留 WORM 保护，即使它们移动到具有 S3 生命周期策略的不同存储类。要跟踪哪些对象具有 S3 对象锁定，您可以参阅包含对象 WORM 状态的 S3 清单报告。S3 对象锁定可以在两种模式之一中配置。部署在监管模式中时，具有特定 IAM 权限的 AWS 账户可以从对象上移除 S3 对象锁定。如果您需要更强的不变性以遵循规章，可以使用合规模式。在合规模式中，任何用户都不能移除保护，包括根账户。

存储监控

在这些管理功能之外，您还可以使用 S3 功能和其他 AWS 服务来监视和控制您的 S3 资源的使用方式。您可以应用标签到 S3 存储桶，以便将成本分配到多个业务维度（例如成本中心、应用程序名称或拥有者），然后使用 AWS 成本分配报告来查看按存储桶标签聚合的使用情况和成本。您还可以使用 Amazon CloudWatch 来跟踪 AWS 资源的运行状况，并配置在估计费用达到用户定义的阈值时发送的账单警报。另一项 AWS 监控服务是 AWS CloudTrail，该服务跟踪并报告存储桶级别和对象级别的活动。您可以配置 S3 事件通知来触发工作流、警报，以及在对 S3 资源进行了特定更改时调用 AWS Lambda。S3 事件通知可用于在媒体文件上传到 Amazon S3 时自动进行转码，在数据文件可用时进行处理，或者与其他数据存储同步对象。

详细了解 S3 存储管理和监控 »

存储类

借助 Amazon S3，您可以在多种不同的 S3 存储类中存储数据：S3 标准、S3 智能分层、Amazon S3 标准 - 不经常访问 (S3 Standard-IA)、S3 单区域 - 不经常访问 (S3 One Zone-IA)、Amazon S3 Glacier (S3 Glacier) 和 Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)。

每个 S3 存储类支持特定的数据访问级别，并具有对应的成本。这意味着您可以将关键任务型生产数据存储在 S3 标准中用于经常访问，将不经常访问的数据存储在 S3 Standard-IA 或 S3 One Zone-IA 中以节省成本，并在成本最低的存档存储类（S3 Glacier 和 S3 Glacier Deep Archive）中存档数据。您可以使用 S3 存储类分析来监控对象的访问模式，用于发现应该移动到较低成本存储类的数据。然后，您可以使用此信息来配置进行数据传输的 S3 生命周期策略。S3 生命周期策略还可用于在数据的生命周期结束时失效这些数据。您可以将访问模式不断变化或未知的数据存储在 S3 智能分层中，这会根据访问模式的变化，自动在经常访问层与较低成本的不经常访问层之间移动数据，从而实现成本节省。

如需了解更多信息，请访问 S3 存储类、S3 存储类分析和 S3 生命周期管理 »

访问管理与安全性

访问管理

为了保护您在 Amazon S3 中的数据，默认情况下用户只有自己所创建 S3 资源的访问权限。您可以使用以下访问管理功能之一或者功能组合来向其他用户授予访问权限：AWS Identity and Access Management (IAM)（创建用户并管理其相应的访问权限）；访问控制列表 (ACL)（使单独的对象可供授权用户访问）；存储桶策略（配置单个 S3 存储桶中所有对象的访问权限）；S3 访问点（通过创建具有名称和每个应用程序或应用程序组特定权限的访问点，简化共享数据集的数据访问管理）；以及查询字符串身份验证（通过临时 URL 向其他用户授予限时访问权限）。Amazon S3 还支持审核日志，其中列出对您 S3 资源发出的请求，从而清楚地了解谁访问了哪些数据。

安全性

Amazon S3 提供了灵活的安全功能，用于阻止未经授权的用户访问数据。使用 VPC 终端节点从您的 Amazon Virtual Private Cloud (Amazon VPC) 连接到 S3 资源。Amazon S3 支持服务器端加密（提供三个密钥管理选项）和用于数据上传的客户端加密。使用 S3 清单可以检查 S3 对象的加密状态（有关 S3 清单的更多信息，请参阅存储管理）。

S3 阻止公有访问是一组安全控制功能，可确保 S3 存储桶和对象不会受到公有访问。只需在 Amazon S3 管理控制台中单击几次，您即可对 AWS 账户内的所有存储桶或特定 S3 存储桶应用 S3 阻止公有访问设置。将设置应用到某个 AWS 账户之后，与该账户关联的任何现有或新的存储桶及对象将继承阻止公有访问的设置。S3 阻止公有访问设置会覆盖其他 S3 访问权限，使账户管理员能够轻松实施“无公有访问”策略，而不管如何添加对象、如何创建存储桶或者是否存在现有的访问权限。S3 阻止公有访问控制是可审核的，这带来更进一步的控制，并可使用

AWS Trusted Advisor 存储桶权限检查、AWS CloudTrail 日志和 Amazon CloudWatch 警报。 您应该为不希望公开访问的所有账户和存储桶启用阻止公有访问。

借助局限于 Virtual Private Cloud (VPC) 的 S3 访问点，您可以在您的私有网络内轻松为您的 S3 数据设置防火墙。此外，您可以使用 AWS 服务控制策略，要求组织中的任何新 S3 访问点仅支持 VPC 访问。

S3 访问分析器功能可以监控您的存储桶访问策略，从而确保策略仅提供对 S3 资源的预期访问。S3 访问分析器可评估您的存储桶访问策略，并使您能够发现并快速修复具有潜在意外访问风险的存储桶。在查看显示对存储桶的潜在共享访问权限的结果时，只需单击 S3 管理控制台，即可阻止所有公共访问存储桶。出于审计目的，可将 S3 访问分析器的结果下载为 CSV 报告。

您可以使用 Amazon Macie 来发现和保护存储在 Amazon S3 中的敏感数据。Macie 可以自动收集完整的 S3 清单，并且持续地评估每个存储桶，以在有任何可公开访问的存储桶、未加密的存储桶或与贵组织之外的 AWS 账户共享或复制的存储桶时发出提醒。然后，Macie 将机器学习和模式匹配技术应用于您选择的存储桶，以识别敏感数据，并向您发出警报，例如个人身份信息 (PII)。安全性结果生成后，它们将被推送到 Amazon CloudWatch Events 之外，这使您可以轻松与现有工作流程系统集成，并使用 AWS Step Functions 等服务触发自动修复，以执行操作，例如关闭公有存储桶或添加资源标签。

如需了解更多信息，请访问 S3 访问管理与安全性和在 Amazon S3 中保护数据 »

随时查询

Amazon S3 具有内置的功能和免费服务，可以查询数据，无需复制并将数据加载到单独的分析平台或数据仓库。这意味着您可以直接对存储在 Amazon S3 中的数据运行大数据分析。S3 Select 是一种为查询设计的 S3 功能，可将查询性能提升高达 400%，并将查询成本减少达 80%。其工作方式是检索某个对象的数据的子集（使用简单 SQL 表达式）而不是整个对象（其大小可高达 5 TB）。

Amazon S3 还与 AWS 分析服务 Amazon Athena 和 Amazon Redshift Spectrum 兼容。Amazon Athena 查询 Amazon S3 中的数据而无需提取数据并加载到单独的服务或平台。它使用标准 SQL 表达式分析数据，在数秒内即可提供结果，通常用于即席数据发现。Amazon Redshift Spectrum 也可直接对 Amazon S3 中的静态数据运行 SQL 查询，更适合较复杂的查询和较大的数据集（可达到 EB 级）。由于 Amazon Athena 和 Amazon Redshift 具有相同的数据目录和数据格式，您可以针对 Amazon S3 中的相同数据集使用它们。

如需更多信息，请访问生成大数据存储解决方案和 S3 Select »

数据传输

AWS 提供数据传输服务组合，从而为任何数据迁移项目提供适当解决方案。连接水平是数据迁移的重大影响因素，AWS 提供可解决您的混合云存储、在线数据传输和离线数据传输需求的产品。

混合云存储：AWS Storage Gateway 是一种混合存储服务，让您可以将本地应用程序无缝连接并扩展到 AWS 存储。客户使用 Storage Gateway 将磁带库无缝替代为云存储，提供云存储支持的文件共享，或创建低延迟缓存来访问 AWS 中本地应用程序的数据。

在线数据传输：AWS DataSync 可以轻松高效地将数百 TB 大小的数百万份文件传输到 Amazon S3 中，速度最高比开源工具快 10 倍。DataSync 可自动处理或消除很多手动任务，包括脚本复制作业、计划和监控传输、验证数据和优化网络利用率。AWS Transfer 系列使用 SFTP、FTPS 和 FTP 提供与 Amazon S3 的完全托管、简单且无缝的文件传输。 Amazon S3 Transfer Acceleration 可在客户与您的 Amazon S3 存储桶之间实现快速的远距离文件传输。

在线数据传输：AWS Snow 系列是专为网络容量受限或不存在的边缘站点构建的服务，可在恶劣的环境中提供存储和计算功能。AWS Snowball 服务使用坚固的便携式存储和边缘计算设备来进行数据收集、处理和迁移。客户可以运送物理 Snowball 设备来进行至 AWS 的离线数据迁移。AWS Snowmobile 是一个 EB 级的数据传输服务，可用于将海量数据移动到云中，包括视频库、图片存储库甚至整个数据中心的迁移。

客户也可以与 AWS 合作伙伴网络 (APN) 中的第三方提供商合作部署混合存储架构、将 Amazon S3 集成到现有应用程序和工作流中，以及在 AWS 云之间往返传输数据。

要了解详情，请访问 AWS 云数据迁移服务 »、AWS Storage Gateway »、AWS DataSync »、AWS Transfer 系列 »、Amazon S3 Transfer Acceleration »、AWS Snow 系列 »