Amazon Simple Storage Service

控制台用户指南

Amazon Simple Storage Service: 控制台用户指南

AWS 文档中描述的 AWS 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 AWS 服务入门。

Table of Contents

本指南不再进行更新。有关当前信息和说明，请参阅新的 Amazon S3 用户指南。

欢迎阅读《Amazon S3 控制台用户指南》

欢迎阅读 Amazon Simple Storage Service (Amazon S3) 控制台的《Amazon Simple Storage Service 控制台用户指南》。

Amazon S3 在 Internet 上提供了近乎无限的存储空间。本指南介绍如何使用 AWS 管理控制台（基于浏览器的图形用户界面）与 AWS 服务交互，从而管理 Amazon S3 中的存储桶、对象和文件夹。

有关 Amazon S3 的工作原理的详细概念信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的什么是 Amazon S3？。本开发人员指南还包含有关 Amazon S3 功能和用于支持这些功能的代码示例的详细信息。

主题

如何更改 AWS 管理控制台的语言？

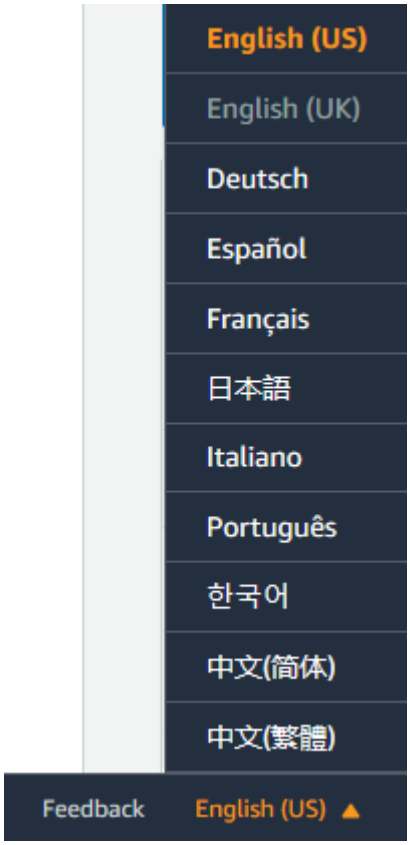
您可以更改 AWS 管理控制台的显示语言。支持多种语言。

更改控制台语言

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在底部导航栏的左侧，选择语言菜单。

3. 从语言菜单中选择所需的语言。

   这将更改整个 AWS 管理控制台的语言。



创建和配置 S3 存储桶

要向 Amazon S3 上传数据（照片、视频、文档等），您必须首先在其中一个 AWS 区域中创建 S3 存储桶。然后，可以将您的数据对象上传到存储桶。

存储于 Amazon S3 中的每个数据元都存储在存储段中。如同通过目录对文件系统中的文件进行分组一样，您也可以使用存储桶对相关对象进行分组。

Amazon S3 在您指定的 AWS 区域中创建存储桶。您可以选择在地理上靠近您的任何 AWS 区域，以便优化延迟，尽可能降低成本或满足法规要求。例如，如果您位于欧洲，您可能会发现在欧洲（爱尔兰）或欧洲（法兰克福）区域创建存储桶十分有利。有关 Amazon S3 AWS 区域的列表，请参阅《Amazon Web Services 一般参考》中的区域和终端节点。

您无需为创建存储桶付费。只有将对象存储到存储桶中以及从存储桶传出对象才需要付费。有关定价的更多信息，请参阅 Amazon Simple Storage Service (S3) 常见问题。

Amazon S3 存储桶名称在全球是唯一的 (无论是在哪个 AWS 区域中创建存储桶)。在创建存储桶时指定名称。有关存储桶命名指南，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储桶限制和局限性。

以下主题介绍如何使用 Amazon S3 控制台创建、删除和管理存储桶。

主题

如何创建 S3 存储桶？

您必须先在某个 AWS 区域中创建用于存储数据的存储桶，然后才能将数据上传到 Amazon S3。创建存储桶后，您可以将无限数量的数据对象上传到该存储桶。

创建存储桶的 AWS 账户拥有该存储桶。默认情况下，您可以在每个 AWS 账户中创建多达 100 个存储桶。如果您需要更多存储桶，则可以通过提交服务配额提升请求将账户的存储桶配额提高至最多 1000 个存储桶。有关如何提升存储桶配额的信息，请参阅《AWS 一般参考》中的 AWS 服务配额。

存储桶具有配置属性，包括地理区域、存储桶中的对象的访问设置以及其他元数据。

创建存储桶

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 选择 Create bucket (创建存储桶)。
3. 在 Bucket name (存储桶名称) 中，输入符合 DNS 标准的存储桶名称。

存储桶名称必须满足以下要求：

- 在所有 Amazon S3 中是唯一的。
- 长度必须介于 3 到 63 个字符之间。
- 不包含大写字符。
- 以小写字母或数字开头。

创建存储桶后，便无法再更改其名称。有关命名存储桶的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储桶命名规则。

> **Important**
>
> 避免在存储桶名称中包含敏感信息，如账号。存储桶名称会显示在指向存储桶中的对象的 URL 中。

4. 在 Region (区域) 中，选择您希望存储桶驻留的 AWS 区域。

   选择一个靠近您的区域可最大程度地减少延迟和成本以及满足法规要求。在某一地区存储的对象将一直留在该地区，除非您特意将其转移到其他地区。有关 Amazon S3 AWS 区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS 服务终端节点。
5. 在 Bucket settings for Block Public Access (阻止公有访问的存储桶设置) 中，选择要应用于存储桶的 Block Public Access (阻止公有访问) 设置。

   我们建议您将所有设置保持为启用状态，除非您知道您需要为您的使用案例关闭其中一个或多个设置，例如托管公共网站。您为存储桶启用的阻止公有访问设置也将为您在存储桶上创建的所有访问点启用。有关阻止公有访问的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 阻止公有访问。
6. （可选）如果要启用 S3 对象锁定：

   a. 选择 Advanced settings (高级设置)，然后阅读显示的消息。

      > **Important**
      >
      > 您只能在创建存储桶时为其启用 S3 对象锁定。如果您为存储桶启用了对象锁定，则以后无法禁用它。启用对象锁定还会启用存储桶的版本控制。为存储桶启用对象锁定后，必须先配置对象锁定设置，然后才能保护存储桶中的任何对象。有关配置对象保护的更多信息，请参阅如何锁定 Amazon S3 对象？ (p. 30)。

   b. 如果要启用对象锁定，请在文本框中输入 enable 并选择 Confirm (确认)。

   有关 S3 对象锁定功能的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 对象锁定以锁定对象。
7. 选择 Create bucket (创建存储桶)。

更多信息

- 如何删除 S3 存储桶？ (p. 4)
- 如何设置 ACL 存储桶权限？ (p. 58)

如何删除 S3 存储桶？

您可以删除空存储桶，并且您在使用 AWS 管理控制台时可以删除包含对象的存储桶。如果删除包含对象的存储桶，则将永久删除该存储桶内的所有对象。

当您删除已启用版本控制的存储桶时，该存储桶中的所有对象的所有版本都将被永久删除。有关版本控制的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的在启用了版本控制的存储桶中管理对象。

在删除存储桶之前，请注意以下事项：

- 存储桶名称是唯一的。如果删除存储桶，则另一个 AWS 用户可以使用该名称。
- 当您删除一个包含对象的存储桶时，该存储桶中的所有对象都将被永久删除，包括已转换为 `S3 Glacier` 存储类的对象。
- 如果该存储桶托管了一个静态网站并且您已按照创建并配置 Amazon Route 53 托管区域中所述创建并配置了 Amazon Route 53 托管区域：您必须按照删除 Route 53 托管区域中所述清理与该存储桶相关的 Route 53 托管区域设置。
- 如果该存储桶收到来自 Elastic Load Balancing (ELB) 的日志数据：建议先停止将 ELB 日志传输到该存储桶，然后再删除该存储桶。删除该存储桶后，如果其他用户创建使用相同名称的存储桶，则日志数据可能会传输到此同名存储桶。有关 ELB 访问日志的信息，请参阅《Classic Load Balancer 用户指南》中的访问日志和《Application Load Balancer 用户指南》中的访问日志。

  Important

  如果您希望继续使用相同的存储桶名称，请不要删除该存储桶。我们建议您，清空并保留存储桶。删除存储桶后，该名称可供重用，但是出于各种原因，您可能无法重新使用该名称。例如，需经过一段时间之后才可再次使用相同名称，而且在您使用该名称之前，其他账户可能会在您之前已使用该名称创建了新存储桶。

删除 S3 存储桶

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要删除的存储桶名称旁边的选项，然后选择页面顶部的 Delete (删除)。
3. 在 Delete bucket (删除存储桶) 页面上，通过在文本字段中输入存储桶名称来确认要删除存储桶，然后选择 Delete bucket (删除存储桶)。

   Note

   如果存储桶包含任何对象，请在删除存储桶之前清空存储桶，具体操作如下：在 This bucket is not empty (此存储桶不为空) 错误提醒中选择 empty bucket configuration (清空存储桶配置) 链接，然后按照 Empty bucket (清空存储桶) 页面上的说明操作。然后，返回到 Delete bucket (删除存储桶) 页面并删除存储桶。

更多信息

- 如何清空 S3 存储桶？ (p. 5)
- 删除对象 (p. 27)

如何清空 S3 存储桶？

您可以清空存储桶，这将删除存储桶中的所有对象而不删除存储桶。在情况已启用版本控制的存储桶时，存储桶中的所有对象的所有版本都将被删除。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的在启用了版本控制的存储桶中管理对象和删除/清空存储桶。

清空 S3 存储桶

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket (存储桶) 列表中，选择要清空的存储桶的名称旁边的选项，然后选择 Empty (清空)。
3. 在 Empty bucket (清空存储桶) 页面上，通过在文本字段中输入 permanently delete (永久删除) 来确认要清空存储桶，然后选择 Empty (清空)。
4. （可选）在 Empty bucket: Status (清空存储桶：状态) 页上监控存储桶清空过程的进度。

Warning

此操作将删除存储桶中的所有对象。等待清空存储桶操作完成，然后添加新对象。如果在清空存储桶操作正在进行时添加新对象，则可能会删除这些对象。

如何查看 S3 存储桶的属性？

您可以查看和配置 Amazon S3 存储桶的属性，包括版本控制、标签、默认加密、日志记录、通知等设置。

查看 S3 存储桶的属性

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要查看其属性的存储桶的名称。
3. 选择属性。
4. 在 Properties 页面上，您可以为存储桶配置以下属性。

   - Bucket Versioning (存储桶版本控制) – 使用版本控制在一个存储桶中保留对象的多个版本。默认情况下，将为新存储桶禁用版本控制。有关启用版本控制的信息，请参阅如何启用或暂停 S3 存储桶的版本控制？
   - Tags (标签) – 利用 AWS 成本分配功能，您可以使用存储桶标签对存储桶的使用计费添加注释。一个标签即为一个键值对，用于表示用户分配给存储桶的标记。要添加标签，请选择 Tags，然后选择 Add tag。有关更多信息，请参阅使用成本分配 S3 存储桶标签。
   - Default encryption (默认加密) – 启用默认加密可为您提供自动服务器端加密。Amazon S3 会在将对象保存到磁盘之前对其进行加密，并在下载对象时对其进行解密。有关更多信息，请参阅 S3 存储桶的 Amazon S3 默认加密。
   - Server access logging (服务器访问日志记录) – 使用服务器访问日志记录详细地记录对您的存储桶提出的各种请求。默认情况下，Amazon S3 不会收集服务器访问日志。有关启用服务器访问日志记录的信息，请参阅如何为 S3 存储桶启用服务器访问日志记录？ (p. 8)。
   - AWS CloudTrail data events (AWS CloudTrail 数据事件) – 使用 CloudTrail 记录数据事件。默认情况下，跟踪不记录数据事件。记录数据事件将收取额外费用。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的记录跟踪的数据事件。
   - Event notifications (事件通知) – 启用特定的 Amazon S3 存储桶事件以在每次发生这些事件时向目标发送通知消息。要启用事件，请选择 Create event notification (创建事件通知)，然后指定要使用的设置。有关更多信息，请参阅 为 S3 存储桶启用和配置事件通知 (p. 16)。
   - Transfer acceleration (传输加速) – 在您的客户端与 S3 存储桶之间实现快速、轻松和安全的远距离文件传输。有关启用传输加速的信息，请参阅如何为 S3 存储桶启用传输加速？ (p. 18)。
   - Object Lock (对象锁定) – 使用 S3 对象锁定在固定的时间段内或无限期地阻止删除或覆盖对象。有关更多信息，请参阅使用 S3 对象锁定来锁定对象。
   - Requester Pays (申请方付款) – 如果您希望申请方（而不是存储桶拥有者）支付请求和数据传输费用，请启用申请方付款。有关更多信息，请参阅申请方付款存储桶。

- Static website hosting (静态网站托管) – 您可以在 Amazon S3 上托管静态网站。要启用静态网站托管，请选择 Static website hosting (静态网站托管)，然后指定要使用的设置。有关更多信息，请参阅如何为静态网站托管配置 S3 存储桶？ (p. 10)。

如何为 S3 存储桶启用或暂停版本控制？

版本控制允许您在一个存储桶中保留多个版本的对象。本节介绍如何在存储桶上启用对象版本控制。有关 Amazon S3 中版本控制支持的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象版本控制和使用版本控制。

在 S3 存储桶上启用或禁用版本控制

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其启用版本控制的存储桶的名称。
3. 选择属性。
4. 在 Bucket Versioning (存储桶版本控制) 下，选择 Edit (编辑)。
5. 选择 Suspend (暂停) 或 Enable (启用)，然后选择 Save changes (保存更改)。

Note

您可以将 AWS Multi-Factor Authentication (MFA) 与版本控制结合使用。将 MFA 与版本控制结合使用时，您必须提供 AWS 账户的访问密钥和账户 MFA 设备中的有效代码，才能永久删除对象版本或暂停或重新激活版本控制。要将 MFA 与版本控制结合使用，请启用 `MFA Delete`。但是，您无法使用 AWS 管理控制台启用 `MFA Delete`。您必须使用 AWS CLI 或 API。有关更多信息，请参阅 MFA 删除。

如何为 Amazon S3 存储桶启用默认加密？

Amazon S3 默认加密提供了一种方法来设置 Amazon S3 存储桶的默认加密行为。您可以对存储桶设置默认加密，以便在存储桶中存储所有对象时对这些对象进行加密。这些对象使用具有 Amazon S3 托管密钥 (SSE-S3) 或 AWS Key Management Service (AWS KMS) 客户主密钥 (CMK) 的服务器端加密进行加密。

在使用服务器端加密时，Amazon S3 在将对象保存到其数据中心的磁盘上之前对其进行加密，并在下载对象时对其进行解密。有关使用服务器端加密和加密密钥管理来保护数据的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用服务器端加密保护数据。

默认加密适用于所有现有的和新的 Amazon S3 存储桶。如果没有默认加密，要对存储在存储桶中的所有对象进行加密，您必须包括加密信息与每个对象存储请求。您还必须设置 Amazon S3 存储桶策略以拒绝不包含加密信息的存储请求。

对 S3 存储桶使用默认加密不会产生新的费用。请求配置默认加密功能会产生标准 Amazon S3 请求费用。有关定价的信息，请参阅 Amazon S3 定价。对于 SSE-KMS CMK 存储，将会产生 AWS KMS 费用，这些费用在 AWS KMS 定价中列出。

对 Amazon S3 存储桶启用默认加密

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择您想要的存储桶的名称。
3. 选择属性。
4. 在 Default encryption (默认加密) 下，选择 Edit (编辑)。
5. 要启用或禁用服务器端加密，请选择 Enable (启用) 或 Disable (禁用)。

6. 要使用 Amazon S3 托管密钥启用服务器端加密，请在 Encryption key type (加密密钥类型) 下，选择 Amazon S3 key (SSE-S3) (Amazon S3 密钥 (SSE-S3))。

   有关使用 Amazon S3 服务器端加密来加密数据的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 托管的加密密钥保护数据。

   Important

   在启用默认加密时，您可能需要更新存储桶策略。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的从使用存储桶策略执行加密转至默认加密。
7. 要使用 AWS KMS CMK 启用服务器端加密，请执行以下步骤：

   a. 在 Encryption key type (加密密钥类型) 下，选择 AWS Key Management Service key (SSE-KMS) (AWS Key Management Service 密钥 (SSE-KMS))。

      Important

      如果您将 AWS KMS 选项用于默认加密配置，则您将受到 AWS KMS 的 RPS（每秒请求数）限制。有关 AWS KMS 限制以及如何请求提高限制的更多信息，请参阅 AWS KMS 限制。

   b. 在 AWS KMS key (AWS KMS 密钥) 下，选择以下选项之一：

      - AWS managed key (aws/s3) (AWS 托管密钥 (aws/s3))
      - Choose from your KMS master keys (从您的 KMS 主密钥中选择)，然后选择 KMS master key (KMS 主密钥)。
      - Enter KMS master key ARN (输入 KMS 主密钥 ARN)，然后输入您的 AWS KMS 密钥 ARN。

      Important

      您只能使用在存储桶所在的 AWS 区域中启用的 KMS CMK。当您选择 Choose from your KMS master keys (从您的 KMS 主密钥中选择) 时，S3 控制台每个区域仅列出 100 个 KMS CMK。如果您在同一区域中有超过 100 个 CMK，则只会在 S3 控制台中看到前 100 个 CMK。若要使用控制台中未列出的 KMS CMK，请选择自定义 KMS ARN，然后输入相应的 KMS CMK ARN。
      当您在 Amazon S3 中使用 AWS KMS CMK 进行服务器端加密时，您必须选择对称 CMK。Amazon S3 仅支持对称 CMK，不支持非对称 CMK。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的使用对称和非对称密钥。

   有关创建 AWS KMS CMK 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥。有关配合使用 AWS KMS 和 Amazon S3 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用存储在 AWS KMS 中的密钥保护数据。
8. 选择保存更改。

更多信息

- 《Amazon Simple Storage Service 开发人员指南》中的 S3 存储桶的 Amazon S3 默认加密
- 如何向 S3 对象添加加密？ (p. 33)

如何为 S3 存储桶启用服务器访问日志记录？

本主题介绍如何使用 AWS 管理控制台为 Amazon S3 存储桶启用服务器访问日志记录。有关以编程方式启用日志记录的信息和有关如何传输日志的详情，请参阅《Amazon Simple Storage Service 开发人员指南》中的服务器访问日志记录。

默认情况下，Amazon Simple Storage Service (Amazon S3) 不会收集服务器访问日志。在您启用日志记录后，Amazon S3 会将源存储桶的访问日志传输到您选择的目标存储桶。目标存储桶必须位于源存储桶所在的相同 AWS 区域中且不得具有默认保留周期配置。

服务器访问日志记录详细地记录对 S3 存储桶提出的各种请求。对于许多应用程序而言，服务器访问日志很有用。例如，访问日志信息可能在安全和访问权限审核方面很有用。它还可以帮助您了解您的客户群并了解您的 Amazon S3 账单。

访问日志记录包含有关对存储桶做出的请求的详细信息。这些信息可能包括请求类型、请求中指定的资源以及处理请求的时间和日期。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的服务器访问日志格式。

> Important
>
> 在 Amazon S3 存储桶上启用服务器访问日志记录不收取额外费用。但是，系统提交给您的任何日志文件都会产生普通存储费用。(您可以随时删除日志文件。) 我们不会计算提交日志文件的数据传输费，但会按正常数据传输费率对访问日志文件收费。

为 S3 存储桶启用服务器访问日志记录

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其启用服务器访问日志记录的存储桶的名称。
3. 选择属性。
4. 在 Server access logging (服务器访问日志记录) 部分中，选择 Edit (编辑)。
5. 在 Server access logging (服务器访问日志记录) 下，选择 Enable (启用)。对于 Target bucket (目标存储桶)，请输入您想要接收日志记录对象的存储桶的名称。目标存储桶必须位于源存储桶所在的相同区域中且不得具有默认保留周期配置。
6. 选择保存更改。

   您可以查看目标存储桶中的日志。启用服务器访问日志记录后，可能需要数小时，日志才会传输到目标存储桶。有关如何以及何时传输日志的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的服务器访问日志记录。

更多信息

如何查看 S3 存储桶的属性？ (p. 6)

如何使用 AWS CloudTrail 数据事件为 S3 存储桶启用对象级别日志记录？

本节描述了如何使用 Amazon S3 控制台启用 AWS CloudTrail 跟踪来记录 S3 存储桶中的对象的数据事件。CloudTrail 支持记录 Amazon S3 对象级别 API 操作，例如 `GetObject`、`DeleteObject` 和 `PutObject`。这些事件称为数据事件。默认情况下，CloudTrail 跟踪不会记录数据事件，但您可以将跟踪配置为记录您指定的 S3 存储桶的数据事件，或记录 AWS 账户中的所有 Amazon S3 存储桶的数据事件。有关更多信息，请参阅使用 AWS CloudTrail 记录 Amazon S3 API 调用。CloudTrail 不会在 CloudTrail 事件历史记录中填充数据事件。此外，并非所有存储桶级别的操作都会填充在 CloudTrail 事件历史记录中。有关更多信息，请参阅使用 Amazon CloudWatch Logs 筛选条件模式和 Amazon Athena 查询 CloudTrail 日志。

要配置跟踪以记录某个 S3 存储桶的数据事件，您可以使用 AWS CloudTrail 控制台或 Amazon S3 控制台。如果您要配置跟踪以记录您的 AWS 账户中所有 Amazon S3 存储桶的数据事件，使用 CloudTrail 控制台会更轻松。有关使用 CloudTrail 控制台配置跟踪以记录 S3 数据事件的信息，请参阅《AWS CloudTrail 用户指南》中的数据事件。

Important

记录数据事件将收取额外费用。有关更多信息，请参阅 AWS CloudTrail 定价。

以下过程演示如何使用 Amazon S3 控制台启用 CloudTrail 跟踪来记录 S3 存储桶的数据事件。

为 S3 存储桶中的对象启用 CloudTrail 数据事件日志记录

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择存储桶的名称。
3. 选择属性。
4. 在 AWS CloudTrail data events (AWS CloudTrail 数据事件) 下，选择 Configure in CloudTrail (在 CloudTrail 中配置)。有关如何在 CloudTrail 控制台中创建跟踪的信息，请参阅《AWS CloudTrail 用户指南》中的使用控制台创建跟踪。
5. 要对存储桶禁用对象级别日志记录，您必须转到 CloudTrail 控制台并从跟踪的 Data events (数据事件) 中删除存储桶名称。

   Note

   如果您使用 CloudTrail 控制台或 Amazon S3 控制台配置某个跟踪以记录 S3 存储桶的数据事件，Amazon S3 控制台将显示已为该存储桶启用对象级别日志记录。

有关创建 S3 存储桶时启用对象级别日志记录的信息，请参阅如何创建 S3 存储桶？ (p. 3)。

更多信息

- 如何查看 S3 存储桶的属性？ (p. 6)
- 《Amazon Simple Storage Service 开发人员指南》中的使用 AWS CloudTrail 记录 Amazon S3 API 调用
- 《AWS CloudTrail 用户指南》中的使用 CloudTrail 日志文件

如何为静态网站托管配置 S3 存储桶？

您可以在 Amazon S3 上托管静态网站。在静态网站上，单独的网页包含静态内容。静态网站可能还包含客户端脚本。通过对比得知，动态网站依赖服务器端处理，包括诸如 PHP、JSP 或 ASP.NET 的服务器端脚本。Amazon S3 不支持服务器端脚本编写。

您可以使用以下快速过程在 Amazon S3 控制台中为静态网站托管配置 S3 存储桶。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的在 Amazon S3 上托管静态网站。有关使用自定义域配置静态网站的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用注册到 Route 53 的自定义域配置静态网站。

主题

步骤 1：为静态网站托管配置存储桶

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在 Buckets (存储桶) 列表中，选择要用于托管静态网站的存储桶的名称。
3. 选择属性。
4. 在 Static website hosting (静态网站托管) 下，选择 Edit (编辑)。
5. 选择 Use this bucket to host a website (使用此存储桶托管网站)。
6. 在 Static website hosting (静态网站托管) 下，选择 Enable (启用)。
7. 在 Index document (索引文档) 中，输入索引文档的文件名，通常为 `index.html`。

   索引文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 索引文档的文件名完全匹配。当您为网站托管配置存储桶时，您必须指定索引文档。当对根域或任何子文件夹发出请求时，Amazon S3 将返回此索引文档。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的配置索引文档。
8. （可选）如果要为 4XX 类错误提供自己的自定义错误文档，请在 Error document (错误文档) 中输入自定义错误文档文件名。

   错误文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 错误文档的文件名完全匹配。如果未指定自定义错误文档并发生错误，Amazon S3 返回默认 HTML 错误文档。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的配置自定义错误文档。
9. （可选）如果要指定高级重定向规则，请在 Redirection rules (重定向规则) 中，输入 XML 来描述规则。

   例如，您可以根据请求中的特定对象键名或前缀按条件路由请求。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的配置高级条件重定向。
10. 选择保存更改。

    Amazon S3 为您的存储桶启用静态网站托管。在页面底部的 Static website hosting (静态网站托管) 下，您可以看到存储桶的网站终端节点。
11. 将索引文档上传到您的存储桶。

    有关将对象上传到 S3 存储桶的分步说明，请参阅通过指向和单击上传文件 (p. 25)。
12. 为您的网站上传其他文件，包括可选的自定义错误文档。

在下一节中，您设置将存储桶作为静态网站进行访问所需的权限。

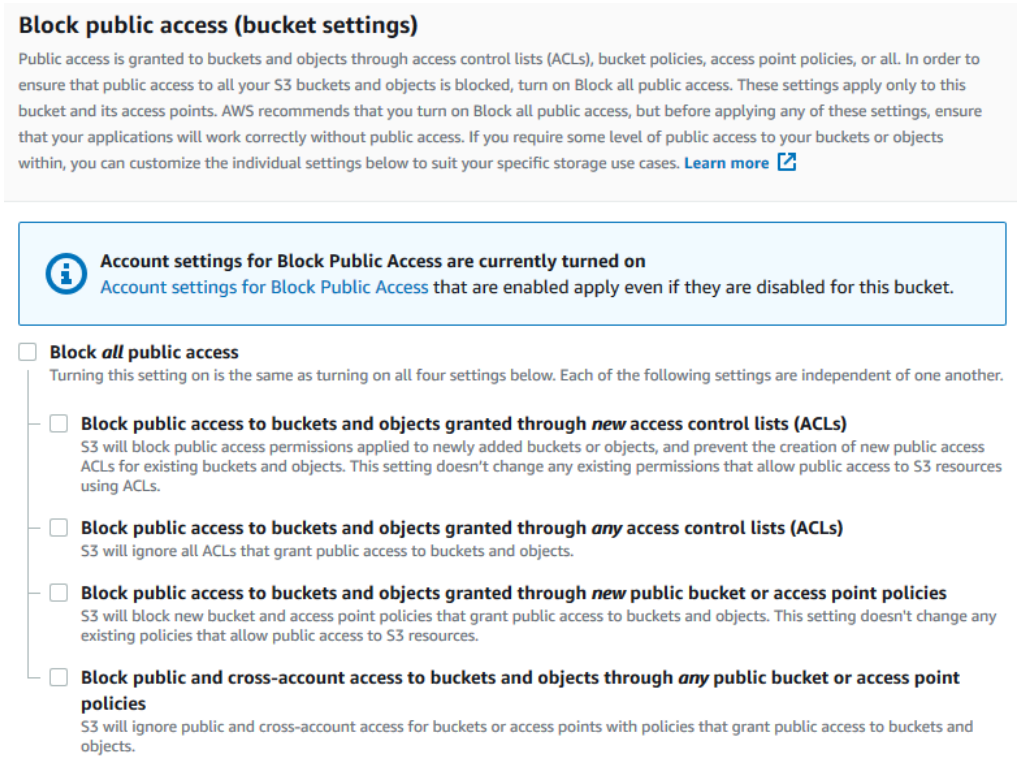
步骤 2：编辑 S3 阻止公有访问设置

默认情况下，Amazon S3 阻止对您的账户和存储桶的公有访问权限。如果要使用存储桶托管静态网站，您可以使用以下步骤编辑您的阻止公有访问设置。

> Warning
>
> 在完成此步骤之前，请查看使用 Amazon S3 阻止公有访问，以确保您了解并接受允许进行公有访问所涉及的风险。当您关闭阻止公有访问设置以使您的存储桶变为公有时，Internet 上的任何人都可以访问您的存储桶。我们建议您阻止对存储桶的所有公有访问。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 选择已配置为静态网站的存储桶的名称。
3. 选择 Permissions。
4. 在 Block public access (bucket settings) (阻止公有访问(存储桶设置)) 下，选择 Edit (编辑)。
5. 清除 Block all public access (阻止所有公有访问)，然后选择 Save changes (保存更改)。

   > Warning
   >
   > 在完成此步骤之前，请查看使用 Amazon S3 阻止公有访问，以确保您了解并接受允许进行公有访问所涉及的风险。当您关闭阻止公有访问设置以使您的存储桶变为公有时，Internet 上的任何人都可以访问您的存储桶。我们建议您阻止对存储桶的所有公有访问。



Amazon S3 关闭了您的存储桶的阻止公有访问设置。要创建公有静态网站，您可能还必须编辑账户的阻止公有访问设置，然后再添加存储桶策略。如果当前已打开账户的阻止公有访问设置，您将在 Block public access (bucket settings) (阻止公有访问(存储桶设置)) 下看到一条备注。

步骤 3：添加存储桶策略

在编辑 S3 阻止公有访问设置后，您可以添加存储桶策略以授予对存储桶的公有读取访问权限。当您授予公有读取访问权限时，Internet 上的任何人都可以访问您的存储桶。

Important

下面的策略仅供举例说明，仍允许完全访问您存储桶的内容。在继续执行此步骤之前，请查看如何保护 Amazon S3 存储桶中的文件？，以确保您了解保护 S3 存储桶中文件的最佳实践以及授予公有访问权限所涉及的风险。

1. 在 Buckets (存储桶) 下，选择存储桶的名称。
2. 选择 Permissions。
3. 在 Bucket Policy (存储桶策略) 下，选择 Edit (编辑)。
4. 要授予对网站的公有读取访问权限，请复制以下存储桶策略，将其粘贴到 Bucket policy editor (存储桶策略编辑器) 中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
```

```
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::example.com/*"
            ]
        }
    ]
}
```

5. 将 `Resource` 更新为您的存储桶名称。

   在前面的示例存储桶策略中，*example.com* 是存储桶名称。要将此存储桶策略用于您自己的存储桶，您必须更新此名称以匹配您的存储桶名称。

6. 选择保存更改。

   此时将显示一条消息，指示存储桶策略已成功添加。

   如果您看到显示 `Policy has invalid resource` 的错误，请确认存储桶策略中的存储桶名称与您的存储桶名称匹配。有关添加存储桶策略的信息，请参阅如何添加 S3 存储桶策略？

   如果您收到错误消息且无法保存存储桶策略，请检查您的账户和存储桶的阻止公有访问设置以确认您允许对存储桶进行公有访问。

在编辑 S3 阻止公有访问设置后，您可以添加存储桶策略以授予对存储桶的公有读取访问权限。当您授予公有读取访问权限时，Internet 上的任何人都可以访问您的存储桶。

Important

下面的策略仅供举例说明，仍允许完全访问您存储桶的内容。在继续执行此步骤之前，请查看如何保护 Amazon S3 存储桶中的文件？，以确保您了解保护 S3 存储桶中文件的最佳实践以及授予公有访问权限所涉及的风险。

步骤 4：测试您的网站终端节点

将存储桶配置为静态网站并设置权限后，您可以通过 Amazon S3 网站终端节点访问您的网站。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的网站终端节点。有关 Amazon S3 网站终端节点的完整列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 网站终端节点。

1. 在 Buckets (存储桶) 下，选择存储桶的名称。
2. 选择属性。
3. 在页面底部的 Static website hosting (静态网站托管) 下，选择 Bucket website endpoint (存储桶网站终端节点)。

   您的索引文档将在单独的浏览器窗口中打开。

如何将对 S3 存储桶托管网站的请求重定向到其他主机？

有关在 Amazon S3 中配置重定向的更多详细信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的配置网页重定向。

您可以将针对存储桶的网站终端节点的所有请求重定向到另一个主机。如果您重定向所有请求，则对网站终端节点所做的任何请求都将重定向至指定的主机名。

例如，如果您的根域为 example.com，并且您要为 http://example.com 和 http://www.example.com 的请求服务，则可以创建两个分别名为 example.com 和 www.example.com 的存储桶。然后，将内容保留在 example.com 存储桶中，然后配置另一个 www.example.com 存储桶以将所有请求重定向至 example.com 存储桶。有关更多信息，请参阅使用自定义域名配置静态网站。

重定向对存储桶网站终端节点的请求

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 下，选择要从中重定向请求的存储桶的名称（例如 www.example.com）。
3. 选择属性。
4. 在 Static website hosting (静态网站托管) 下，选择 Edit (编辑)。
5. 选择 Redirect requests for an object (重定向对于对象的请求)。
6. 在 Host name (主机名) 框中，输入存储桶或自定义域的网站终端节点。

   例如，如果您正在重定向到根域地址，则输入 **example.com**。
7. 对于 Protocol (协议)，选择重定向请求的协议（none (无)、http 或 https）。

   如果未指定协议，则默认选项为 none (无)。
8. 选择 Save changes。

S3 存储桶属性的高级设置

此部分介绍如何为标签、对象复制和事件通知和传输加速配置高级 S3 存储桶属性设置。

主题

- 设置目标以接收 Amazon S3 事件通知 (p. 14)
- 为 S3 存储桶启用和配置事件通知 (p. 16)
- 如何为 S3 存储桶启用传输加速？ (p. 18)

设置目标以接收 Amazon S3 事件通知

在为存储桶启用事件通知之前，必须设置以下目标类型之一。

目标类型

- Amazon SNS 主题 (p. 14)
- Amazon SQS 队列 (p. 15)
- Lambda 函数 (p. 15)

Amazon SNS 主题

Amazon Simple Notification Service (Amazon SNS) 是一项 Web 服务，用于协调和管理向订阅终端节点或客户端交付或发送消息的过程。您可以使用 Amazon SNS 控制台创建 Amazon SNS 主题以便向其发送通知。Amazon SNS 主题必须与您的 Amazon S3 存储桶位于同一区域。有关创建 Amazon SNS 主题的信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的入门和 SNS 常见问题。

您先需要以下内容，然后才能将创建的 Amazon SNS 主题用作事件通知目标：

- Amazon SNS 主题的 Amazon 资源名称 (ARN)

- 一个有效的 Amazon SNS 主题订阅（主题订阅者在消息发布到 Amazon SNS 主题时会收到通知）
- 您在 Amazon SNS 控制台中设置的一个权限策略（如以下示例所示）

```
{
  "Version":"2012-10-17",
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SNS:Publish",
      "Resource":"arn:aws:sns:region:account-number:topic-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

Amazon SQS 队列

Amazon Simple Queue Service (Amazon SQS) 提供可靠且可扩展的托管队列，用于在消息在计算机之间传输时存储消息。您可以使用 Amazon SQS 控制台创建 Amazon SQS 队列以便向其发送通知。Amazon SQS 队列必须与您的 Amazon S3 存储桶位于同一区域。有关创建 Amazon SQS 队列的信息，请参阅《Amazon Simple Queue Service 开发人员指南》中的什么是 Amazon Simple Queue Service 和 Amazon SQS 入门。

您先需要以下内容，然后才能使用 Amazon SQS 队列作为事件通知目标：

- Amazon SQS 主题的 Amazon 资源名称 (ARN)
- 您在 Amazon SQS 控制台中设置的一个权限策略（如以下示例所示）

```
{
  "Version":"2012-10-17",
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SQS:*",
      "Resource":"arn:aws:sqs:region:account-number:queue-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

Lambda 函数

您可以使用 AWS Lambda 控制台创建使用 AWS 基础设施代表您运行代码的 Lambda 函数。Lambda 函数必须与您的 S3 存储桶位于同一区域。您还必须具有 Lambda 函数的名称或 ARN 才能将 Lambda 函数设置为事件通知目标。

Warning

如果您的通知最终写入触发通知的存储桶，这可能会导致执行循环。例如，如果每当上传一个对象，存储桶就触发某个 Lambda 函数，而该函数又上传一个对象给存储桶，则该函数间接触发了自身。为避免这种情况，请使用两个存储桶，或将触发器配置为仅适用于传入对象所用的前缀。
有关将 Amazon S3 通知与 AWS Lambda 结合使用的更多信息和示例，请参阅《AWS Lambda 开发人员指南》中的结合使用 AWS Lambda 和 Amazon S3。

有关向 Amazon S3 授予向目标发布事件通知所需的权限的更多信息，请参阅《Amazon S3 开发人员指南》中的授予将事件通知消息发布到目标的权限。

为 S3 存储桶启用和配置事件通知

您可以启用特定的 Amazon S3 事件，以便每次发生这些事件时都向目标发送通知消息。本部分介绍了如何使用 Amazon S3 控制台启用事件通知。有关将事件通知与 AWS 开发工具包和 Amazon S3 REST API 配合使用的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的配置 Amazon S3 事件通知。

主题

事件通知类型

为存储桶配置事件通知时，您必须指定要接收其通知的事件类型。有关事件类型的完整列表，请参阅《Amazon Simple Storage Service 开发人员指南》中的支持的事件类型部分。

在 Amazon S3 控制台中，提供了以下用于配置事件通知的选项。可以选择一个选项或多个选项。

- 对象创建
  - All object create events (所有对象创建事件) – 通过以下任何对象创建操作在您的存储桶中创建对象时收到通知：Put (放置)、Post (发布)、Copy (复制) 和 Multipart upload completed (分段上传已完成)。
  - Put (放置)、Post (发布)、Copy (复制) 和 Multipart upload completed (分段上传已完成) – 收到有关这些特定对象创建操作之一的通知。
- 删除对象
  - All object delete events (所有对象删除事件) – 只要删除存储桶中的对象，就会收到通知。
  - Delete marker created (已创建删除标记) – 为受版本控制的对象创建删除标记时收到通知。

    有关删除受版本控制的对象的信息，请参阅删除对象版本。有关对象版本控制的信息，请参阅对象版本控制和使用版本控制。
- 从 S3 Glacier 或 S3 Glacier Deep Archive 存储类还原对象
  - Restore initiated (已启动还原) – 启动 对象还原时收到通知。
  - Restore completed (已完成还原) – 对象还原完成 时收到通知。
- 低冗余存储 (RRS) 对象丢失事件
  - Object in RSS Lost (RSS 中的对象丢失) – RRS 存储类的对象丢失时收到通知
- 能够使用 Amazon S3 复制时间控制执行复制的对象
  - Replication time missed threshold (复制时间未达到阈值) – 收到有关对象复制时间超过 15 分钟阈值的通知。
  - Replication time completed after threshold (复制时间在阈值后完成) – 收到有关对象在 15 分钟阈值后复制的通知。
  - Replication time not tracked (未跟踪复制时间) – 收到有关复制指标不再跟踪符合复制条件的对象的通知。
  - Replication time failed (复制时间失败) – 收到有关对象无法复制的通知。

Note

当您从文件夹中删除最后一个对象时，Amazon S3 会生成对象创建事件。如果有多个前缀相同的对象的尾随斜杠 (/) 是其名称的一部分，则这些对象在 Amazon S3 控制台中将显示为文件夹的一部分。文件夹的名称由尾随斜杠 (/) 前面的字符构成。
如果删除该文件夹下列出的所有对象，则不提供任何实际对象来表示空文件夹。在这种情况下，Amazon S3 控制台会创建一个零字节对象来表示该文件夹。如果您启用了对象创建的事件通知，则由控制台执行的零字节对象创建操作会触发对象创建事件。
Amazon S3 控制台在以下情况下显示文件夹：

- 当零字节对象的名称中包含尾随斜杠 (/) 时。在这种情况下，有一个 0 字节的实际 Amazon S3 对象用于表示文件夹。
- 如果对象名称中包含一个斜杠 (/)。在这种情况下，没有代表该文件夹的实际对象。

启用和配置事件通知

您必须先设置其中一个目标类型，然后才能为存储桶启用事件通知。有关更多信息，请参阅 设置目标以接收 Amazon S3 事件通知 (p. 14)。

为 S3 存储桶启用和配置事件通知

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其启用事件的存储桶的名称。
3. 导航到 Event Notifications (事件通知) 部分，然后选择 Create event notification (创建事件通知)。
4. 在 General configuration (常规配置) 部分中，为事件通知指定描述性事件名称。您还可以选择指定前缀和后缀，以将通知限制为键以指定字符结尾的对象。

   a. 为 Event name (事件名称) 输入描述。

      如果未输入名称，则将生成一个全局唯一标识符 (GUID) 并用作名称。

   b. 要选择按前缀筛选事件通知，请输入 Prefix (前缀)。

      例如，可以设置前缀筛选器，使得仅在文件添加到特定文件夹（例如 `images/`）时，您才会收到通知。

   c. 要选择按后缀筛选事件通知，请输入 Suffix (后缀)。

      有关更多信息，请参阅使用对象键名筛选配置通知。
5. 在 Event types (事件类型) 部分中，选择要接收其通知的一个或多个事件类型。

   有关事件类型的列表，请参阅事件通知类型 (p. 16)。
6. 在 Destination (目标) 部分中，选择事件通知目标。

   Note

   在发布事件通知之前，您必须向 Amazon S3 委托人授予调用相关 API 以将通知发布到 Lambda 函数、SNS 主题或 SQS 队列的必要权限。

   a. 选择目标类型：Lambda Function (Lambda 函数)、SNS Topic (SNS 主题) 或 SQS Queue (SQS 队列)。
   b. 选择目标类型后，从下拉列表中选择函数、主题或队列。
   c. 或者，如果您希望指定 Amazon 资源名称 (ARN)，请选择 Enter ARN (输入 ARN) 并输入 ARN。

   有关更多信息，请参阅 设置目标以接收 Amazon S3 事件通知 (p. 14)。
7. 选择 Save changes (保存更改)，Amazon S3 会向事件通知目标发送一条测试消息。

有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的配置 Amazon S3 事件通知。

如何为 S3 存储桶启用传输加速？

Amazon Simple Storage Service (Amazon S3) 传输加速可在您的客户端与 S3 存储桶之间实现快速、轻松、安全的远距离文件传输。本主题介绍如何为存储桶启用 Amazon S3 Transfer Acceleration。有关更多信息，请参阅 Amazon Simple Storage Service 开发人员指南中的 Amazon S3 传输加速。

> Note
>
> 如果要比较加快的上传速度与未加快的上传速度，请打开 Amazon S3 Transfer Acceleration 速度比较工具。
> 此速度比较工具使用分段上传来将文件从浏览器传输到各种使用和未使用 Amazon S3 Transfer Acceleration 的 AWS 区域。您可以比较直接上传和按区域传输加速上传的上传速度。

为 S3 存储桶启用传输加速

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，选择要为其启用加速传输的存储桶的名称。
3. 选择属性。
4. 在 Transfer acceleration (传输加速) 下，选择 Edit (编辑)。
5. 选择 Enable (启用)，然后选择 Save changes (保存更改)。

   Amazon S3 为您的存储桶启用 Transfer Acceleration，并显示存储桶的 Properties (属性) 选项卡。在 Transfer acceleration (传输加速) 下，Accelerated endpoint (加速终端节点) 显示存储桶的传输加速终端节点。可以使用此终端节点访问与存储桶之间的加速数据传输。如果您暂停传输加速，加速终端节点不再起作用。

Amazon S3 访问点简介

您可以使用 Amazon S3 访问点来管理对 S3 对象的访问。Amazon S3 访问点是附加到存储桶的命名网络终端节点，您可以使用它们执行 S3 对象操作（例如上传和检索对象）。存储桶最多可附加 1,000 个访问点，并且每个访问点都强制实施不同的权限和网络控制，从而让您可以精细地控制 S3 对象的访问。

有关 Amazon S3 访问点的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 访问点管理数据访问。

以下主题介绍如何使用 S3 管理控制台创建、管理和使用 Amazon S3 访问点。

主题

创建 Amazon S3 访问点

本节介绍如何通过 AWS 管理控制台来创建 Amazon S3 访问点。有关使用 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 创建访问点的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 访问点管理数据访问。

一个访问点只与一个 Amazon S3 存储桶相关联。在开始之前，请确保已创建要与此访问点一起使用的存储桶。有关创建存储桶的更多信息，请参阅创建和配置 S3 存储桶 (p. 3)。

创建访问点

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在控制台左侧的导航窗格中，选择 Access points (访问点)。
3. 在访问点页面上，选择 Create access point (创建访问点)。
4. 在 Access point name (访问点名称) 字段中输入期望的访问点名称。有关命名访问点的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的命名 Amazon S3 访问点的规则。
5. 在 Bucket name (存储桶名称) 字段中，输入账户中要将访问点附加到的存储桶的名称，例如 `DOC-EXAMPLE-BUCKET1`。或者，您可以选择 Browse S3 (浏览 S3) 以浏览和搜索账户中的存储桶。如果选择 Browse S3 (浏览 S3)，请选择所需的存储桶，然后选择 Choose path (选择路径) 以使用该存储桶的名称填充 Bucket name (存储桶名称) 字段。
6. （可选）选择 View (查看) 以在新的浏览器窗口中查看指定存储桶的内容。
7. 选择 Network origin (网络源)。如果您选择 Virtual private cloud (VPC)，请输入要与访问点一起使用的 VPC ID。

   有关访问点的网络源的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的创建限制到 Virtual Private Cloud 的访问点。
8. 在 Access point settings for Block Public Access (阻止公有访问的访问点设置) 下，选择要应用于访问点的阻止公有访问设置。默认情况下，为新访问点启用所有阻止公有访问设置，我们建议您保持启用所有设置，除非您有特定的需求要禁用它们中的任何一个设置。Amazon S3 当前不支持在创建访问点之后更改访问点的阻止公有访问设置。

   有关使用 Amazon S3 阻止访问点的公有访问的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的管理访问点的公有访问。

9. （可选）在 Access point policy (访问点策略) - optional (可选) 下，指定访问点策略。有关指定访问点策略的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问点策略示例。
10. 选择 Create access point (创建访问点)。

管理和使用 Amazon S3 访问点

本节介绍如何通过 AWS 管理控制台来管理和使用 Amazon S3 访问点。在开始之前，请导航至要管理或使用的访问点的详细信息页面，如以下程序中所述。

导航到访问点详细信息页面

选项 1：列出账户的所有访问点

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在控制台左侧的导航窗格中，选择 Access points (访问点)。
3. 在 Access points (访问点) 页面的 Access points (访问点) 下面，选择包含待列出的访问点的 AWS 区域。
4. （可选）通过在“Region (区域)”下拉菜单旁边的文本字段中输入名称，按名称搜索访问点。
5. 选择要管理或使用的访问点的名称。

选项 2：列出单个存储桶的所有访问点

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在控制台左侧的导航窗格中，选择 Buckets (存储桶)。
3. 在 Buckets (存储桶) 页面上，选择要列出其访问点的存储桶的名称。
4. 在存储桶详细信息页面上，选择 Access points (访问点) 选项卡。
5. 选择要管理或使用的访问点的名称。

管理和使用单个访问点

查看访问点的配置详细信息

1. 导航到要查看其详细信息的访问点的详细信息页面，如导航到访问点详细信息页面 (p. 20)中所述。
2. 在 Access point overview (访问点概述) 下，查看所选访问点的配置详细信息和属性。

使用访问点来访问存储桶

1. 导航到要使用的访问点的详细信息页面，如导航到访问点详细信息页面 (p. 20)中所述。
2. 在 Objects (对象) 选项卡下，选择要通过访问点访问的一个或多个对象的名称。在对象操作页面上，控制台在存储桶名称上方显示一个标签，该标签显示您当前正在使用的访问点。在使用访问点时，您只能执行访问点权限允许的对象操作。

   Note

   - 控制台视图始终显示存储桶中的所有对象。如本过程中所述使用访问点会限制您可以对这些对象执行的操作，但不会限制您是否能够看到这些对象存在于存储桶中。
   - S3 管理控制台不支持使用 Virtual Private Cloud (VPC) 访问点访问存储桶资源。要从 VPC 访问点访问存储桶资源，请使用 AWS CLI、AWS 开发工具包或 Amazon S3 REST API。

查看访问点的“阻止公有访问”设置

1. 导航到要查看其设置的访问点的详细信息页面，如导航到访问点详细信息页面 (p. 20)中所述。
2. 选择 Permissions。
3. 在 Access point policy (访问点策略) 下，查看访问点的阻止公有访问设置。

   Note

   创建访问点后，您无法更改访问点的阻止公有访问设置。

编辑访问点策略

1. 导航到要编辑其策略的访问点的详细信息页面，如导航到访问点详细信息页面 (p. 20)中所述。
2. 选择 Permissions。
3. 在 Access point policy (访问点策略) 下，选择 Edit (编辑)。
4. 在文本字段中输入访问点策略。控制台会自动显示访问点的 Amazon 资源名称 (ARN)，您可以在策略中使用该名称。
5. 选择 Save。

删除访问点

1. 导航到您的账户或特定存储桶的访问点列表，如导航到访问点详细信息页面 (p. 20)中所述。
2. 选择要删除的访问点名称旁边的选项按钮。
3. 选择 Delete。
4. 在显示的文本字段中输入访问点名称，然后选择 Delete (删除)，确认您要删除访问点。

上传、下载和管理对象

要向 Amazon S3 上传数据（照片、视频、文档等），您必须首先在其中一个 AWS 区域中创建 S3 存储桶。您随后可以将无限数量的数据对象上传到该存储桶。

您存储在 Amazon S3 中的数据包含对象。所有对象都位于您在特定 AWS 区域中创建的存储桶内。存储在 Amazon S3 中的所有对象都位于存储桶内。

在某一区域存储的对象将一直留在该区域，除非您特意将其传输到另一区域。例如，在欧洲（爱尔兰）区域存储的对象将一直留在欧洲。在某个 AWS 区域中存储的对象会议物理形式保留在该区域。Amazon S3 不会保留这些对象的副本或将其移动到其他任何区域。但是，只要您具有执行此操作的必要权限，就可以从任何地方访问这些对象。

您必须先拥有存储段写入权限，才能将数据元上传到 Amazon S3 中。

对象可以是任何类型的文件：图像、备份、数据和电影等。一个存储桶中可以有无限量的对象。可使用 Amazon S3 控制台上传的文件的最大大小为 160 GB。要上传大于 160 GB 的文件，请使用 AWS CLI、AWS 开发工具包或 Amazon S3 REST API。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的上传对象。

以下主题介绍如何使用 Amazon S3 控制台上传、删除和管理对象。

> Note
>
> 如果重命名对象或更改存储类、加密或元数据属性，则将创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色还会成为新对象或（对象版本）的拥有者。

主题

如何将文件和文件夹上传至 S3 存储桶？

本主题介绍如何使用 AWS 管理控制台将一个或多个文件或整个文件夹上传至 Amazon S3 存储桶。您需要拥有存储桶写入权限，才能将文件和文件夹上传至 Amazon S3 存储桶。有关访问权限的更多信息，请参阅设

置存储桶和对象访问权限 (p. 54)。有关以编程方式上传文件的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的上传对象。

在您将文件上传至 Amazon S3 时，文件会被存储为 S3 对象。对象由文件数据和描述对象的元数据组成。一个存储桶中可以有无限量的对象。

您可以将任何类型的文件上传至 S3 存储桶，包括映像、备份、数据、电影等。可使用 Amazon S3 控制台上传的文件的最大大小为 160 GB。要上传大于 160 GB 的文件，请使用 AWS CLI、AWS 开发工具包或 Amazon S3 REST API。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的上传对象。

> Note
>
> 要上传文件夹，则必须使用拖放方式。要上传文件，可以拖放文件或指向并单击文件。只有 Chrome 和 Firefox 浏览器支持拖放功能。

有关受支持 Chrome 和 Firefox 浏览器版本的信息，请参阅支持哪些浏览器与 AWS 管理控制台一起使用？

上传文件夹时，Amazon S3 会将所有文件和子文件夹从指定文件夹中上传至存储桶。然后，它会分配由上传文件名和文件夹名组成的对象键名。例如，如果您上传包含 `sample1.jpg` 和 `sample2.jpg` 这两个文件的名为 `/images` 的文件夹，则 Amazon S3 会上传这两个文件，然后分配相应的键名 `images/sample1.jpg` 和 `images/sample2.jpg`。键名包括作为前缀的文件夹名。Amazon S3 控制台仅显示最后一个“/”后面的键名部分。例如，在图像文件夹中，`images/sample1.jpg` 和 `images/sample2.jpg` 对象显示为 `sample1.jpg` 和 `sample2.jpg`。

如果您上传单个文件并且您在 Amazon S3 控制台中打开了一个文件夹，那么在上传文件时，Amazon S3 会将打开的文件夹的名称包含在内，作为键名的前缀。例如，如果您在 Amazon S3 控制台中打开了一个名为 `backup` 的文件夹，则您上传的名为 `sample1.jpg` 的文件的键名为 `backup/sample1.jpg`。但是在控制台中，对象在 `sample1.jpg` 文件夹中显示为 `backup`。

如果您上传单个文件并且您在 Amazon S3 控制台中没有打开文件夹，那么在上传文件时，Amazon S3 仅会将文件名指定为键名。例如，如果您上传的文件名为 `sample1.jpg`，则键名为 `sample1.jpg`。有关键名的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象键和元数据。

如果启用了版本控制的存储桶中已存在所上传对象的键名，则 Amazon S3 会创建该对象的另一个版本，而不是替换现有对象。有关版本控制的更多信息，请参阅如何为 S3 存储桶启用或暂停版本控制？ (p. 7)。

主题

使用拖放功能上传文件和文件夹

如果您使用的是 Chrome 或 Firefox 浏览器，则您可以选择要上传的文件夹和文件，然后将其拖放到目标存储桶中。拖放是上传文件夹的唯一方式。

使用拖放功能将文件夹和文件上传到 S3 存储桶

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要将文件夹和文件上传到的存储桶的名称。
3. 在控制台窗口以外的窗口中，选择要上传的文件和文件夹。然后，将您选择的内容拖放到列出目标存储桶中对象的控制台窗口。

   Upload (上传) 页面上将列出所选文件。

4. 在 Upload (上传) 页面上，您可以将更多文件和文件夹拖放到显示 Upload (上传) 页面的控制台窗口中。要添加更多文件，您还可以选择 Add files (添加文件) 或 Add folder (添加文件夹)。
5. 在 Destination (目标) 部分中，如果未启用版本控制，则必须选中确认将覆盖具有相同名称的对象的复选框。

   要立即上传列出的文件和文件夹，而无需授予或解除特定用户的权限或为您正在上传的所有文件设置公共权限，请选择页面底部的 Upload (上传)。有关对象访问权限的信息，请参阅 如何在对象上设置权限？ (p. 57)。
6. 在 Storage class (存储类) 部分中，为要上传的文件选择存储类。有关存储类的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储类。
7. 为正在上传的文件选择加密类型。如果您不想加密，请选择 Disable (禁用)。

   a. 要使用由 Amazon S3 托管的密钥加密上传的文件，请选择 Amazon S3 key (Amazon S3 密钥)。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 托管的加密密钥类保护数据。

   b. 要使用 AWS Key Management Service (AWS KMS) 加密上传的文件，请选择 AWS Key Management Service key (AWS Key Management Service 密钥)。然后，从 AWS KMS CMK 列表中选择客户主密钥 (CMK)。

      Note

      要加密存储桶中的对象，您只能使用存储桶所在相同 AWS 区域提供的 CMK。

      您可以授权外部账户使用由 AWS KMS CMK 保护的对象。为此，请从列表中选择 Custom KMS ARN，然后输入外部账户的 Amazon 资源名称 (ARN)。如果外部账户管理员对由您的 AWS KMS CMK 保护的对象有使用权限，则可通过创建资源级 IAM 策略来进一步限制访问权限。

      有关创建 AWS KMS CMK 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥。有关使用 AWS KMS 保护数据的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用存储在 AWS KMS (SSE-KMS) 中的密钥保护数据。
8. 在 Access control list (ACL) (访问控制列表 (ACL)) 部分中，您可以更改 AWS 账户拥有者的权限。owner (拥有者) 是指 AWS 账户根用户，而不是 AWS Identity and Access Management (IAM) 用户。有关根用户的更多信息，请参阅 AWS 账户根用户。

   您可以向一般公众（世界上的每一个人）授予对您的对象的读取访问权限，使其能够获取您正在上传的所有文件。授予公有读取访问权限适用于一小部分的用例 (如存储桶用于网站时)。建议您不要更改默认设置。您始终可以在上传对象后更改对象权限。有关对象访问权限的信息，请参阅 如何在对象上设置权限？ (p. 57)。

   选择 Add grantee (添加被授权者) 可向其他 AWS 账户授予访问权限。有关向其他 AWS 账户授予权限的更多信息，请参阅如何设置 ACL 存储桶权限？ (p. 58)。
9. 对象标签为您提供了对存储进行分类的方法。每个标签都是一个键-值对。键和标签值区分大小写。对于每个对象，您最多可以有 10 个标签。

   要向上传的所有对象添加标签，请选择 Add tag (添加标签)。在 Key (键) 字段中键入标签名称。键入标签的值。标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 255 个 Unicode 字符。有关对象标签的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象标签。
10. Amazon S3 对象的元数据由一个名称-值（键-值）对表示。有两种元数据：系统定义的元数据和用户定义的元数据。要将元数据添加到要上传的所有对象中，请选择 Add Metadata (添加元数据)。

    a. 如果要添加 Amazon S3 系统定义的元数据，对于 Type (类型)，请选择 System Defined (系统定义)。对于 Key (键)，选择一个键。您可以选择通用的 HTTP 标头，如 Content-Type 和 Content-Disposition。键入该键的值。有关系统定义的元数据的列表，以及有关您是否可以添加其值的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的系统定义的元数据。

    b. 以前缀 `x-amz-meta-` 开头的任何元数据都被视为用户定义的元数据。用户定义元数据会与对象存储在一起，并会在您下载该对象时返回。

要将用户定义的元数据添加到所有正在上传的对象中，对于 Type (类型)，请选择 User Defined (用户定义)。在 Key (键) 字段中键入 `x-amz-meta-` 加上自定义元数据名称。键入该键的值。密钥及其值均必须符合 US-ASCII 标准。用户定义元数据最大可为 2 KB。有关用户定义的元数据的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的用户定义的元数据。

11. 选择 Upload。

通过指向和单击上传文件

此过程介绍如何通过选择 Upload 将文件上传到 S3 存储桶。

通过指向和单击将文件上传到 S3 存储桶

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要将文件上传到的存储桶的名称。
3. 选择 Upload。
4. 在 Upload (上传) 页面上，选择 Add files (添加文件) 或 Add folder (添加文件夹)。
5. 选择要上传的一个或多个文件，然后选择 Open。
6. 在您看到 Upload (上传) 对话框中列出了您选择的文件后，请继续执行 使用拖放功能上传文件和文件夹 (p. 23) 的步骤 5：

更多信息

- 如何在对象上设置权限？ (p. 57)。
- 如何从 S3 存储桶下载对象？ (p. 26)

复制对象

在 Amazon S3 控制台中，您可以将对象复制到同一 AWS 区域内的存储桶或访问点。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制对象。

复制对象

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 导航到包含待复制对象的 Amazon S3 存储桶或文件夹。
3. 选中要复制的对象名称左侧的复选框。
4. 选择 Actions (操作)，然后从显示的选项列表中选择 Copy (复制)。

   或者，从右上角的选项中选择 Copy (复制)。
5. 选择目标类型和目标账户。要指定目标路径，请选择 Browse S3 (浏览 S3)，导航到目标，然后选中目标左侧的复选框。选择右下角的 Choose destination (选择目标)。

   或者，输入目标路径。
6. 如果未启用存储桶版本控制，则系统可能会要求您确认是否覆盖具有相同名称的现有对象。如果可以覆盖，请选中该复选框并继续。如果要在此存储桶中保留对象的所有版本，请选择 Enable Bucket Versioning (启用存储桶版本控制)。您还可以更新默认加密和对象锁定属性。
7. 选择右下角的 Copy (复制)，Amazon S3 会将您的对象移动到目标位置。

Note

- 此操作创建具有更新设置的所有指定对象的副本，更新指定位置的上次修改日期，然后向原始对象添加删除标记。
- 移动文件夹时，请等待移动操作完成，然后再对文件夹进行其他更改。
- 无法使用 S3 控制台复制使用客户提供的加密密钥 (SSE-C) 加密的对象。要复制使用 SSE-C 加密的对象，请使用 AWS CLI、AWS 开发工具包或 Amazon S3 REST API。
- 此操作会更新存储桶版本控制、加密、对象锁定功能和存档对象的元数据。

移动对象

在 Amazon S3 控制台中，您可以将对象移动到存储桶或文件夹中。

移动对象

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 导航到包含待移动对象的 Amazon S3 存储桶或文件夹。
3. 选中要移动的对象名称左侧的复选框。
4. 选择 Actions (操作)，然后从显示的选项列表中选择 Move (移动)。

   或者，从右上角的选项中选择 Move (移动)。
5. 要指定目标路径，请选择 Browse S3 (浏览 S3)，导航到目标，然后选中目标左侧的复选框。选择右下角的 Choose destination (选择目标)。

   或者，输入目标路径。
6. 如果未启用存储桶版本控制，则系统可能会要求您确认是否覆盖具有相同名称的现有对象。如果可以覆盖，请选中该复选框并继续。如果要在此存储桶中保留对象的所有版本，请选择 Enable Bucket Versioning (启用存储桶版本控制)。您还可以更新默认加密和对象锁定属性。
7. 选择右下角的 Move (移动)，Amazon S3 会将您的对象移动到目的地。

Note

- 此操作创建具有更新设置的所有指定对象的副本，更新指定位置的上次修改日期，然后向原始对象添加删除标记。
- 移动文件夹时，请等待移动操作完成，然后再对文件夹进行其他更改。
- 无法使用 S3 控制台复制使用客户提供的加密密钥 (SSE-C) 加密的对象。要复制使用 SSE-C 加密的对象，请使用 AWS CLI、AWS 开发工具包或 Amazon S3 REST API。
- 此操作会更新存储桶版本控制、加密、对象锁定功能和存档对象的元数据。

如何从 S3 存储桶下载对象？

本部分介绍如何使用 Amazon S3 控制台从 S3 存储桶下载对象。

下载对象时需收取数据传输费。有关 Amazon S3 功能和定价的信息，请参阅 Amazon S3。

Important

- 如果对象键包含单个句点 (.) 或两个句点 (..)，您将无法使用 Amazon S3 控制台下载该对象。要下载键名为“.”或“..”的对象，您必须使用 AWS CLI、AWS 开发工具包或 REST API。有关命名对象的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象键命名指引。

- 您可以使用 Amazon S3 控制台为每个请求下载一个对象。要下载多个对象，请使用 AWS CLI、AWS 开发工具包或 REST API。

从 S3 存储桶下载对象

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要从中下载对象的存储桶的名称。
3. 您可以使用以下任一方式从 S3 存储桶下载对象：
   - 选择要下载的对象的名称。

     在 Overview 页面上，选择 Download。
   - 选择要下载的对象的名称，然后从 Action (操作) 菜单中选择 Download (下载) 或 Download as (下载方式)。
   - 选择要下载的对象的名称。选择 Latest version，然后选择下载图标。

相关主题

- 如何将文件和文件夹上传至 S3 存储桶？ (p. 22)

删除对象

本部分介绍如何使用 Amazon S3 控制台删除对象。由于 S3 存储桶中的所有对象都会产生存储费用，因此您应从中删除不再需要的对象。例如，如果您正在收集日志文件，最好在不再需要这些文件时将其删除。您可以将生命周期规则设置为自动删除对象 (如日志文件)。有关生命周期规则的更多信息，请参阅本指南中的如何为 S3 存储桶创建生命周期规则？ (p. 41)。

有关 Amazon S3 功能和定价的信息，请参阅 Amazon S3。

删除对象

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 导航到包含待删除对象的 Amazon S3 存储桶或文件夹。
3. 选中要删除的对象名称左侧的复选框。
4. 选择 Actions (操作)，然后从显示的选项列表中选择 Delete (删除)。

   或者，从右上角的选项中选择 Delete (删除)。
5. 如果系统要求您确认删除这些对象，请输入 **`delete`**。
6. 选择右下角的 Delete objects (删除对象)，Amazon S3 会删除指定的对象。

   Warning

   - 删除指定的对象无法撤销。
   - 此操作将删除所有指定的对象。删除文件夹时，请等待删除操作完成，然后再将新对象添加到文件夹。否则，新对象也可能会被删除。
   - 删除指定的对象无法撤销。

如何取消删除已删除的 S3 对象？

本部分介绍如何使用 Amazon S3 控制台恢复（取消删除）已删除的对象。

为了能够取消删除已删除的对象，您必须在该对象被删除前已在包含该对象的存储桶上启用版本控制。有关启用版本控制的信息，请参阅如何为 S3 存储桶启用或暂停版本控制？ (p. 7)。

当您删除启用了版本控制的存储桶中的某个对象时，所有版本都将保留在存储桶中并且 Amazon S3 将为该对象创建一个删除标记。要取消删除该对象，您必须删除此删除标记。有关版本控制和删除标记的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象版本控制。

从 S3 存储桶恢复已删除的对象

以下步骤描述了如何从 S3 存储桶中恢复文件夹之外的已删除对象，包括这些文件夹中的对象。

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择您想要的存储桶的名称。
3. 要查看存储桶中对象的版本列表，请选择 List versions (列出版本) 开关。您将能够看到已删除对象的删除标记。
4. 要取消删除对象，您必须删除掉删除标记。选中要恢复的对象的删除标记旁边的复选框，然后选择 Delete (删除)。
5. 在 Delete objects (删除对象) 页面上确认删除。

   a. 在 Pemanently delete objects? (永久删除对象？) 下输入 **`permanently delete`**。
   b. 选择 Delete objects (删除对象)。

   Note

   您无法使用 Amazon S3 控制台取消删除文件夹。您必须使用 AWS CLI 或开发工具包。例如，请参阅如何检索启用版本控制的存储桶中已被删除的 Amazon S3 对象？

更多信息

- 如何查看 S3 对象的版本？ (p. 31)
- 如何为 S3 存储桶启用或暂停版本控制？ (p. 7)
- 《Amazon Simple Storage Service 开发人员指南》中的使用版本控制

如何还原已存档的 S3 对象？

此部分介绍如何使用 Amazon S3 控制台还原已存档到 S3 Glacier 或 S3 Glacier Deep Archive 存储类的对象。无法立即访问存储在 S3 Glacier 或 S3 Glacier Deep Archive 中的对象。要访问此类别中的对象，必须首先在您指定的持续时间（天数）内将对象的临时副本还原到其 S3 存储桶。有关 S3 Glacier 或 S3 Glacier Deep Archive 存储类的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储类。

在还原存档时，您需要为存档和已还原的副本付费。由于副本有存储成本，因此请仅在您需要的时间段还原对象。如果您想获得对象的永久拷贝，可在 S3 存储桶中创建该对象的拷贝。有关 Amazon S3 功能和定价的信息，请参阅 Amazon S3。

对象还原后，您可以从 Overview 页面中下载。有关更多信息，请参阅如何查看对象概述？ (p. 31)。

主题

档案检索选项

以下是还原已归档对象时可用的检索选项：

- **`Expedited`** - 加速检索允许您在偶尔需要紧急请求存档子集时快速访问存储在 S3 Glacier 存储类中的数据。对于除最大存档对象 (250 MB+) 之外的所有其他存档对象，使用加速检索访问的数据通常在 1 到 5 分钟内可用。预配置容量确保在您需要时，可以使用针对加速检索的检索容量。有关更多信息，请参阅预配置容量。存储在 S3 Glacier Deep Archive 存储类中的对象无法使用加速检索和预配置容量。
- **`Standard`** - 标准检索允许您在数小时内访问您的任何存档对象。这是未指定检索选项的 S3 Glacier 和 S3 Glacier Deep Archive 检索请求的默认选项。对于存储在 S3 Glacier 存储类中的对象，标准检索通常在 3-5 小时内完成。对于存储在 S3 Glacier Deep Archive 存储类中的对象，检索通常在 12 小时内完成。
- **`Bulk`** - 批量检索是 Amazon S3 Glacier 中成本最低的检索选项，使您可以以较低的成本检索大量（甚至是 PB 级）的数据。对于存储在 S3 Glacier 存储类中的对象，批量检索通常在 5-12 小时内完成。对于存储在 S3 Glacier Deep Archive 存储类中的对象，检索通常在 48 小时内完成。

有关检索选项的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的还原存档对象。

恢复已存档的 S3 对象

此主题介绍如何使用 Amazon S3 控制台还原已存档到 S3 Glacier 或 S3 Glacier Deep Archive 存储类的对象。（控制台使用 Glacier 和 Glacier Deep Archive 作为这些存储类的名称。）

恢复已存档的 S3 对象

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择包含您想要还原的对象的存储桶的名称。
3. 在 Name (名称) 列表中，选择要还原的一个或多个对象，再选择 Actions (操作)，然后选择 Initiate restore (启动还原)。
4. 在启动还原对话框中，键入您希望存档数据可访问的天数。
5. 使用检索选项菜单在下列检索选项中的选择一个选项。
   - 选择批量检索或标准检索l，然后选择还原。
   - 选择 Expedited retrieval (加速检索)（仅适用于 Glacier 存储类）。
6. 预配置的容量仅对 Glacier 存储类可用。如果您有预配置容量，请选择 还原以开始进行预配置检索。如果您有预配置容量，则您的预配置容量可处理您的所有加速检索。有关预配置容量的更多信息，请参阅预配置容量。
   - 如果您没有预配置容量并且不想购买，请选择还原。
   - 如果您没有预配置容量但是想要购买，请选择添加容量单位，然后选择购买。在收到购买成功消息后，选择还原开始预配置检索。

升级正在进行的还原

在还原过程中，您可以升级还原的速度。

将正在进行的还原升级到更快的层级

1. 在名称列表中，选择正在还原的一个或多个对象，再选择操作，然后选择从 Glacier 还原。有关检查对象还原状态的信息，请参阅检查存档还原状态和到期日期 (p. 30)。
2. 选择要升级到的层级，然后选择还原。有关升级到更快的还原层级的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的还原存档对象。

检查存档还原状态和到期日期

要检查还原进度，请查看对象概述面板。有关概述面板的信息，请参阅 如何查看对象概述？ (p. 31)。

概览部分显示还原正在进行。

当对象的临时副本可用后，对象的概览部分将显示恢复过期日期。此时 Amazon S3 将删除您的存档的已还原副本。

系统只会在您指定的天数内存储已恢复的对象。如果您想获得对象的永久拷贝，可在 Amazon S3 存储桶中创建该对象的拷贝。

Amazon S3 通过将您指定的天数与您请求还原对象的时间相加来计算过期日期，然后四舍五入至 UTC 时间第二天的午夜。该计算方法既适用于对象的初始恢复，也适用于您请求的所有可用时间延期。例如，如果对象的恢复时间为 2012/10/15 10:30 AM UTC 且您指定的天数为 3 天，则该对象在 2012/10/19 00:00 UTC 前均可用。如果您在 10/16/2012 11:00 AM UTC 将您希望的可访问天数更改为 1，则 Amazon S3 会将还原对象的可用截止日期更改为 10/18/2012 00:00 UTC。

对象还原后，您可以从 Overview 页面中下载。有关更多信息，请参阅如何查看对象概述？ (p. 31)。

更多信息

- 《Amazon S3 开发人员指南》中的还原已存档的对象。
- AWS CLI 命令参考中的 restore-object。
- 《S3 Glacier 开发人员指南》中的 Amazon S3 Glacier 中的 Identity and Access Management。
- 如何为 S3 存储桶创建生命周期规则？ (p. 41)
- 如何取消删除已删除的 S3 对象？ (p. 28)

如何锁定 Amazon S3 对象？

借助 S3 对象锁定，您可以使用一次写入，多次读取 (WORM) 模式在 Amazon S3 中存储对象。您可以使用 S3 对象锁定在固定的时间段内或无限期地阻止删除或覆盖对象。有关使用 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 锁定对象的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用对象锁定来锁定对象。

在锁定任何对象之前，您必须允许存储桶使用 S3 对象锁定。您可在创建存储桶时启用对象锁定。对存储桶启用对象锁定后，便可锁定该存储桶中的对象。如果您创建存储桶时启用了对象锁定，您将无法为该存储桶禁用对象锁定或暂停版本控制。

有关在启用 S3 对象锁定的情况下创建存储桶的信息，请参阅如何创建 S3 存储桶？ (p. 3)。

锁定 Amazon S3 对象

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择您想要的存储桶的名称。

3. 在 Objects (对象) 列表中，选择要锁定的对象的名称。
4. 选择属性。
5. 选择对象锁定。
6. 选择一种保留模式。您可以更改保留到期日期。您也可以选择启用 Legal hold (依法保留)。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 S3 对象锁定概述。
7. 选择 Save。

更多信息

- 设置存储桶和对象访问权限 (p. 54)

如何查看对象概述？

本节介绍如何使用 Amazon S3 控制台查看对象概述面板。此面板在一个位置概述了对象的所有基本信息。

查看对象的概述面板

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket (存储桶) 列表中，选择包含对象的存储桶的名称。
3. 在 Name (名称) 列表中，选中要查看其概述的对象名称旁边的复选框。
4. 要下载对象，请选择对象概述面板中的 Download。要将对象的路径复制到剪贴板，请选择 Copy Path。
5. 如果对存储桶启用了版本控制，请选择 Latest versions 以列出对象的版本。然后，您可以选择下载图标以下载对象版本，或选择垃圾桶图标以删除对象版本。

   Important

   仅当对象已作为最新 (当前) 版本删除时，您才能取消删除它。您无法取消删除已删除对象的早期版本。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象版本控制和使用版本控制。

更多信息

- 如何查看 S3 对象的版本？ (p. 31)

如何查看 S3 对象的版本？

本节介绍如何使用 Amazon S3 控制台查看对象的不同版本。

启用了版本控制的存储桶可以具有同一对象的多个版本：一个当前 (最新) 版本和零个或零个以上非当前 (早期) 版本。Amazon S3 会对每个数据元分配具有唯一性的版本 ID。有关启用版本控制的信息，请参阅如何为 S3 存储桶启用或暂停版本控制？ (p. 7)。

如果存储桶已启用版本控制，则 Amazon S3 将在以下条件下创建对象的另一个版本：

- 如果您上传的对象与存储桶中已存在的某个对象同名，则 Amazon S3 会创建对象的另一个版本，而不是替换现有对象。

- 如果您在将对象上传到存储桶之后更新了任何对象属性（如更改存储详细信息或其他元数据），Amazon S3 将在存储桶中创建一个新的对象版本。

有关 Amazon S3 中版本控制支持的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象版本控制和使用版本控制。

查看对象的多个版本

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket (存储桶) 列表中，选择包含对象的存储桶的名称。
3. 要查看存储桶中对象的版本列表，请选择 List versions (列出版本) 开关。

   控制台会显示每个对象版本的唯一版本 ID、对象版本的创建日期和时间以及其他属性。(在您设置版本控制状态之前存储在存储桶中的对象具有版本 ID null。)

   要列出没有版本的对象，请选择 List versions (列出版本) 开关。

您也可以在对象概述面板中查看、下载和删除对象版本。有关更多信息，请参阅 如何查看对象概述？ (p. 31)。

> **Important**
>
> 仅当对象已作为最新 (当前) 版本删除时，您才能取消删除它。您无法取消删除已删除对象的早期版本。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象版本控制和使用版本控制。

更多信息

- 如何为 S3 存储桶启用或暂停版本控制？ (p. 7)
- 如何为 S3 存储桶创建生命周期规则？ (p. 41)

如何查看对象的属性？

本部分介绍如何使用控制台查看对象的属性。

查看对象的属性

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket (存储桶) 列表中，选择包含对象的存储桶的名称。
3. 在 Name 列表中，选择要查看其属性的对象的名称。
4. 选择属性。
5. 在 Properties 页面上，您可以为对象配置以下属性。

   > **Note**
   >
   > 如果更改存储类、加密或元数据属性，则将创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色还会成为新对象或（对象版本）的拥有者。

   a. Storage class (存储类) – Amazon S3 中的每个对象都有与之关联的存储类。您选择使用的存储类取决于您访问对象的频率。S3 对象的默认存储类是 STANDARD。您可以选择在上传对象使用的存储

类。有关存储类的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储类。

要在上传对象后更改存储类，请选择 Storage class。选择您希望的存储类，然后选择 Save。

b. Encryption (加密) – 您可以加密您的 S3 对象。有关更多信息，请参阅如何向 S3 对象添加加密？ (p. 33)。
c. Metadata (元数据) – Amazon S3 中的每个对象都有一组表示其元数据的名称/值对。有关将元数据添加到 S3 对象的信息，请参阅 编辑对象元数据 (p. 34)。
d. Tags (标签) – 您可以将标签添加至 S3 对象。有关更多信息，请参阅编辑对象标签 (p. 36)。
e. Object lock (对象锁定) – 您可以防止删除对象。

如何向 S3 对象添加加密？

本主题描述如何使用 Amazon S3 控制台设置或更改对象的加密类型。

Note

如果更改对象的加密，则会创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色也会成为新对象或（对象版本）的拥有者。

添加或更改对象的加密

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket (存储桶) 列表中，选择包含对象的存储桶的名称。
3. 在 Name (名称) 列表中，选择要为其添加或更改加密的对象的名称。
4. 选择 Properties，然后选择 Encryption。

   此时将打开加密对话框，为您提供三种对象加密选择：

   - None (无) - 无对象加密。
   - AES-256 - 具有 Amazon S3 托管密钥的服务器端加密 (SSE-S3)。
   - AWS-KMS - 具有 AWS Key Management Service (AWS KMS) 客户主密钥的服务器端加密 (SSE-KMS)。
5. 如果要从已有加密设置的对象中删除加密，请依次选择无和保存。
6. 如果要使用由 Amazon S3 托管的密钥加密对象，请按照下列步骤操作：

   a. 选择 AES-256。

      有关使用 Amazon S3 服务器端加密来加密数据的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 托管的加密密钥类保护数据。
   b. 选择 Save。
7. 如果要使用 AWS KMS 加密对象，请按照下列步骤操作：

   a. 选择 AWS-KMS。
   b. 选择 AWS KMS 客户主密钥 (CMK)。

      该列表显示您创建的客户托管 CMK 和 Amazon S3 的 AWS 托管 CMK。有关创建客户托管 AWS KMS CMK 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥。

      Important

      Amazon S3 控制台只为每个 AWS 区域列出 100 个 AWS KMS CMK。如果您在同一区域中有超过 100 个 CMK，您只会在 S3 控制台中看到前 100 个 CMK。若要使用控制台中未列出的 KMS CMK，请选择自定义 KMS ARN，然后输入相应的 KMS CMK ARN。

c. 选择 Save。

Important

要加密存储桶中的对象，您只能使用存储桶所在相同 AWS 区域启用的 CMK。Amazon S3 仅支持对称 CMK。注意：Amazon S3 不支持非对称 CMK。有关更多信息，请参阅使用对称和非对称密钥。

8. 要授权外部账户使用由 AWS KMS CMK 保护的对象，请按照以下步骤操作：

a. 选择 AWS-KMS。
b. 输入外部账户的 Amazon 资源名称 (ARN)。
c. 选择 Save。

如果外部账户管理员对由您的 AWS KMS CMK 保护的对象有使用权限，则可通过创建资源级 AWS Identity and Access Management (IAM) 策略来进一步限制访问权限。

Note

此操作将加密应用于所有指定的对象。加密文件夹时，请等待保存操作完成，然后再将新对象添加到文件夹。

更多信息

- 如何为 Amazon S3 存储桶启用默认加密？ (p. 7)
- 《Amazon Simple Storage Service 开发人员指南》中的 S3 存储桶的 Amazon S3 默认加密
- 如何查看对象的属性？ (p. 32)
- 上传、下载和管理对象 (p. 22)

编辑对象元数据

本节介绍如何使用 Amazon S3 控制台编辑现有 S3 对象的元数据。Amazon S3 中的每个对象都可以具有一组键值对来提供元数据，这是有关该对象的附加信息。在您上传对象时，Amazon S3 会设置一些元数据。例如，`Content-Length` 是键（名称），值 是对象的大小（以字节为单位）。

您也可以在上传对象时设置一些元数据，并稍后在需求更改时对其进行编辑。例如，您可能有一组初始存储在 `STANDARD` 存储类中的对象。随着时间的推移，您可能不再需要此数据具有高可用性，并通过将 `x-amz-storage-class` 键的值从 `STANDARD` 编辑为 `GLACIER` 来将存储类更改为 `GLACIER`。

S3 对象有两种元数据，即 Amazon S3 系统定义的 元数据和用户定义的 元数据：

- 系统定义的元数据 – 在系统元数据中，有两种类别。
  - 诸如 `Last-Modified` 日期之类的元数据由系统控制，只有 Amazon S3 可以修改该值。
  - 还有您可以修改的系统元数据，例如，对象的存储类或加密类型。
- 用户定义的元数据 – 您可以定义自己的自定义元数据，称为用户定义的元数据，在您上传对象时或对象已上传后将这种元数据分配给对象。用户定义元数据会与对象存储在一起，并会在您下载该对象时返回。Amazon S3 不处理用户定义的元数据。

以下主题介绍了如何使用 Amazon S3 控制台编辑对象的元数据。

主题

- 编辑系统定义的元数据 (p. 35)

- 编辑用户定义的元数据 (p. 35)

Note

- 此操作将使用更新的设置和上次修改日期创建对象的副本。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的 IAM 角色还会成为新对象或（对象版本）的拥有者。
- 编辑元数据会更新现有键名的值。
- 使用客户提供的加密密钥 (SSE-C) 加密的对象无法使用控制台进行复制，必须使用 AWS CLI、AWS 开发工具包或 Amazon S3 REST API。

Warning

- 编辑文件夹的元数据时，请等待编辑元数据操作完成，然后再将新对象添加到文件夹。否则，也可能会编辑新对象。
- 使用客户提供的加密密钥 (SSE-C) 加密的对象无法使用控制台进行复制，必须使用 AWS CLI、AWS 开发工具包或 Amazon S3 REST API。

有关对象元数据的更多信息（包括命名准则和限制），请参阅《Amazon Simple Storage Service 开发人员指南》中的对象元数据。

编辑系统定义的元数据

您可以为 S3 对象配置某些（但并非全部）系统元数据。有关系统定义的元数据的列表以及您是否可以修改其值，请参阅《Amazon Simple Storage Service 开发人员指南》中的系统定义的元数据。

编辑对象的系统定义的元数据

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 导航到您的 Amazon S3 存储桶或文件夹，然后选中要编辑其元数据的对象名称左侧的复选框。
3. 打开 Action (操作) 菜单，转到 Edit actions (编辑操作) 部分，然后选择 Edit metadata (编辑元数据)。
4. 查看列出的对象，然后选择 Add metadata (添加元数据)。
5. 对于元数据 Type (类型)，请选择 System-defined (系统定义)。
6. 指定唯一的 Key (键) 和元数据 Value (值)。
7. 要编辑其他元数据，请选择 Add metadata (添加元数据)。您还可以选择 Remove (删除) 以删除一组类型-键-值。
8. 完成后，选择 Save changes (保存更改)，Amazon S3 将编辑指定对象的元数据。

编辑用户定义的元数据

您可以通过组合元数据前缀 `x-amz-meta-` 和选择用于创建自定义键的名称来编辑对象的用户定义的元数据。例如，如果您添加自定义名称 `alt-name`，则元数据键为 `x-amz-meta-alt-name`。用户定义元数据最大可为 2 KB。键及其值均必须符合 US-ASCII 标准。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的用户定义的元数据。

编辑对象的用户定义的元数据

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 导航到您的 Amazon S3 存储桶或文件夹，然后选中要编辑其元数据的对象名称左侧的复选框。
3. 打开 Action (操作) 菜单，转到 Edit actions (编辑操作) 部分，然后选择 Edit metadata (编辑元数据)。
4. 查看列出的对象，然后选择 Add metadata (添加元数据)。
5. 对于元数据 Type (类型)，请选择 User-defined (用户定义)。
6. 在 `x-amz-meta-` 后面输入唯一的自定义 Key (键)。还输入元数据 Value (值)。
7. 要添加其他元数据，请选择 Add metadata (添加元数据)。您还可以选择 Remove (删除) 以删除一组类型-键-值。
8. 完成后，选择 Save changes (保存更改)，Amazon S3 将编辑指定对象的元数据。

更多信息

- 如何查看对象的属性？ (p. 32)
- 上传、下载和管理对象 (p. 22)

编辑对象标签

对象标签为您提供了对存储进行分类的方法。本主题介绍上传对象之后如何使用控制台向 S3 对象添加标签。有关在上传对象时向对象添加标签的信息，请参阅如何将文件和文件夹上传至 S3 存储桶？ (p. 22)。

每个标签都是遵循以下规则的键值对：

- 您最多可以将 10 个标签与对象关联。与对象关联的标签必须具有唯一的标签键。
- 标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 256 个 Unicode 字符。
- 键和标签值区分大小写。

有关对象标签的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象标签。有关标签限制的更多信息，请参阅《AWS 账单和成本管理用户指南》中的用户定义的标签限制。

向对象添加标签

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 导航到您的 Amazon S3 存储桶或文件夹，然后选中要向其添加标签的对象名称左侧的复选框。
3. 打开 Action (操作) 菜单，转到 Edit actions (编辑操作) 部分，然后选择 Edit Tags (编辑标签)。
4. 查看列出的对象，然后选择 Add tags (添加标签)。
5. 每个对象标签都是一个键值对。输入 Key (键) 和 Value (值)。要添加另一个标签，请选择 Add Tag (添加标签)。完成后，选择 Save changes (保存更改)，然后 Amazon S3 将标签添加到指定的对象。

   您最多可以为一个对象输入 10 个标签。

有关更多信息，另请参阅本指南中的 如何查看对象的属性？ (p. 32) 和 上传、下载和管理对象 (p. 22)。

如何在 S3 存储桶中使用文件夹？

在 Amazon S3 中，存储桶和对象是主要资源，并且对象存储在存储桶中。Amazon S3 具有扁平结构，而不是类似于您在文件系统中看到的层次结构。不过，为了实现组织简易性，Amazon S3 控制台支持将文件夹概

念作为对象分组手段。Amazon S3 通过为对象（即名称以通用字符串开头的对象）使用共享名称前缀来实现这一点。对象名称也称为键名称。

例如，您可以在控制台中创建名为 `photos` 的文件夹，并在其中存储名为 `myphoto.jpg` 的对象。随后，将使用键名 `photos/myphoto.jpg` 存储对象，其中 `photos/` 为前缀。

以下是另外两个示例：

- 如果您的存储桶中有三个对象 `logs/date1.txt`、`logs/date2.txt` 和 `logs/date3.txt`，则控制台会显示名为 `logs` 的文件夹。如果您在控制台中打开该文件夹，将看到三个对象：`date1.txt`、`date2.txt` 和 `date3.txt`。
- 如果您有名为 `photos/2017/example.jpg` 的对象，则控制台会显示名为 `photos` 的文件夹，其中包含文件夹 `2017` 和对象 `example.jpg`。

主题

文件夹中可以有文件夹，但存储桶中不能有存储桶。可以直接将对象上传和复制到一个文件夹中。可以创建和删除文件夹以及将文件夹设为公用，但不能对文件夹进行重命名。可以将对象从一个文件夹复制至另一个文件夹。

> **Important**
>
> - Amazon S3 控制台通过创建以文件夹前缀和分隔符值作为键的零字节对象来实现文件夹对象创建。这些文件夹对象不会显示在控制台中。否则，它们的行为与任何其他对象一样，可以通过 REST API、AWS CLI 和 AWS 开发工具包进行查看和操作。
> - 对于将正斜杠“/”字符作为键名称中的最后一个（尾部）字符的所有对象（例如 `examplekeyname/`），Amazon S3 控制台将其视为文件夹。您无法使用 Amazon S3 控制台上传键名称中有尾部“/”字符的对象。但是，通过使用 AWS CLI、AWS 开发工具包或 REST API，您可以利用 Amazon S3 API 上传名称中有尾部“/”的对象。
> - 名称中有尾部“/”的对象显示为 Amazon S3 控制台中的文件夹。Amazon S3 控制台不为此类对象显示内容和元数据。当使用控制台复制名称中有尾部“/”的对象时，将在目标位置创建一个新文件夹，但不会复制对象的数据和元数据。

创建文件夹

本部分介绍如何使用 Amazon S3 控制台创建文件夹。

> **Important**
>
> 如果存储桶策略阻止在没有加密、标签、元数据或访问控制列表 (ACL) 被授权者的情况下将对象上传到此存储桶，则您将无法使用此配置创建文件夹。请改为上传空文件夹并在上传配置中指定这些设置。

如何创建文件夹

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要在其中创建文件夹的存储桶的名称。
3. 选择 Create folder。
4. 输入文件夹的名称（例如，**`favorite-pics`**）。单击 Create folder (创建文件夹)。

如何从 S3 存储桶中删除文件夹？

本节介绍如何使用 Amazon S3 控制台从 S3 存储桶中删除文件夹。

有关 Amazon S3 功能和定价的信息，请参阅 Amazon S3。

从 S3 存储桶中删除文件夹

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要从中删除文件夹的存储桶的名称。
3. 在 Name (名称) 列表中，选中要删除的文件夹和对象旁边的复选框，选择 Actions (操作)，然后选择 Delete (删除)。
4. 在 Delete objects (删除对象) 页面上，验证是否已列出选择删除的文件夹的名称。在提供的框中输入 **`delete`**，然后单击 Delete objects (删除对象)。

   Warning

   此操作将删除所有指定的对象。删除文件夹时，请等待删除操作完成，然后再将新对象添加到文件夹。否则，新对象也可能会被删除。

相关主题

- 删除对象 (p. 27)

将文件夹设为公用

Amazon S3 具有扁平结构，而不是类似于您通常在文件系统中看到的层次结构。不过，为了实现组织简易性，Amazon S3 控制台支持将文件夹概念作为对象分组手段。在 Amazon S3 中，文件夹是一个对象或一组对象的命名前缀。有关更多信息，请参阅 如何在 S3 存储桶中使用文件夹？ (p. 36)。

我们建议禁止所有对 Amazon S3 文件夹和存储桶的公有访问，除非您特别需要公有文件夹或存储桶。当您将文件夹设为公有时，Internet 上的任何人都可以查看该文件夹中分组的所有对象。在 Amazon S3 控制台中，您可以将文件夹设为公有。您还可以通过创建存储桶策略来将文件夹设为公有，该策略通过前缀限制访问。有关更多信息，请参阅 设置存储桶和对象访问权限 (p. 54)。

Warning

在 Amazon S3 控制台中将文件夹设为公有后，就不能再将其设为私有。而是必须对公有文件夹中的每个单独的对象设置权限，以使对象不具备公有访问。有关更多信息，请参阅 如何在对象上设置权限？ (p. 57)。

更多信息

- 如何从 S3 存储桶中删除文件夹？ (p. 38)
- 如何设置 ACL 存储桶权限？ (p. 58)
- 如何对 S3 存储桶阻止公有访问？ (p. 55)

S3 批量操作简介

S3 批量操作对 Amazon S3 对象执行大规模批量操作。您可以使用 S3 批量操作复制对象、设置对象标签或访问控制列表 (ACL)、从 Amazon S3 Glacier 中启动对象还原或调用 AWS Lambda 函数以使用您的对象执行自定义操作。您可以对自定义的对象列表执行这些操作，也可以使用 Amazon S3 清单报告来轻松生成最大的对象列表。S3 批量操作使用以前使用的 Amazon S3 API 来调用这些操作，因此您会发现界面很熟悉。有关使用 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 执行 S3 批量操作的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的执行 S3 批量操作。

以下主题介绍如何使用 Amazon S3 控制台配置和运行批量操作。

主题

创建 S3 批处理操作作业

本部分介绍如何创建 S3 批处理操作作业。有关使用 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 执行批处理操作的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的执行 S3 批处理操作。

创建批量作业

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Amazon S3 控制台的导航窗格中选择 Batch Operations (批处理操作)。
3. 选择创建作业。
4. 选择要在其中创建作业的 Region (区域)。
5. 在 Manifest format (清单格式) 下，选择要使用的清单对象的类型。
   - 如果您选择 S3 inventory report (S3 清单报告)，请输入 Amazon S3 在 CSV 格式的清单报告中生成的 manifest.json 对象的路径，以及（可选）输入清单对象的版本 ID（如果您要使用的版本不是最新版本）。
   - 如果您选择 CSV，请输入 CSV 格式清单对象的路径。清单对象必须遵循控制台中描述的格式。如果您希望使用并非最新的对象版本，则可以选择包含清单对象的版本 ID。
6. 选择 Next (下一步)。
7. 在 Operation (操作) 下，选择您希望对清单中列出的所有对象执行的操作。填写您所选操作的信息，然后选择下一步。
8. 填写配置额外选项的信息，然后选择下一步。
9. 对于审核，验证设置。如果需要进行更改，请选择 Previous。否则，选择创建作业。

更多信息

- 《Amazon Simple Storage Service 开发人员指南》中的基础知识：S3 批处理操作作业
- 《Amazon Simple Storage Service 开发人员指南》中的创建 S3 批处理操作作业
- 《Amazon Simple Storage Service 开发人员指南》中的操作

管理 S3 批处理操作作业

Amazon S3 提供一组功能强大的工具，帮助您在创建 S3 批处理操作作业后管理作业。有关管理 S3 批处理操作的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的管理 S3 批处理操作作业。

更多信息

- 《Amazon Simple Storage Service 开发人员指南》中的基础知识：S3 批处理操作作业
- 《Amazon Simple Storage Service 开发人员指南》中的创建 S3 批处理操作作业
- 《Amazon Simple Storage Service 开发人员指南》中的操作

存储管理

本部分介绍如何配置 Amazon S3 存储管理工具。

主题

如何为 S3 存储桶创建生命周期规则？

您可以使用生命周期规则来定义您希望 Amazon S3 在对象的生命周期内执行的操作（例如，将对象转化为另一个存储类别、检索它们或在指定时期后删除它们）。

您可以使用共享前缀（以通用字符串开头的对象名称）或标签为存储桶中的所有对象或一部分对象定义生命周期规则。

使用生命周期规则，您可以定义特定于当前和非当前对象版本的操作。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象生命周期管理、对象版本控制和使用版本控制。

创建生命周期规则

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其创建生命周期规则的存储桶的名称。
3. 选择 Management (管理) 选项卡，然后选择 Create lifecycle rule (创建生命周期规则)。
4. 在 Lifecycle rule name (生命周期规则名称) 中，输入规则的名称。

   在该存储桶内，此名称必须是唯一的。
5. 选择生命周期规则的范围：

   - 要将此生命周期规则应用于所有带特定前缀或标签的对象，请选择将范围限制在特定前缀或标签。
     - 要按前缀限制范围，请在 Prefix (前缀) 中输入前缀。
     - 要按标签限制范围，请选择 Add tag (添加标签)，然后输入标签键和值。

     有关对象名称前缀的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象键。有关对象标签的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象标签。

- 要将此生命周期规则应用于存储桶中的所有对象，请选择 This rule applies to all objects in the bucket (此规则适用于存储桶中的所有对象)，然后选择 I acknowledge that this rule applies to all objects in the bucket (我确认此规则适用于存储桶中的所有对象)。

6. 在 Lifecycle rule actions (生命周期规则操作) 下，选择希望生命周期规则执行的操作：

   - 在存储类之间转换对象的当前版本
   - 在存储类之间转换对象的先前版本
   - 使对象的当前版本过期
   - 永久删除对象的先前版本
   - 删除过期的删除标记或未完成的分段上传

   根据您选择的操作，会显示不同的选项。

7. 要在存储类之间转换对象的当前版本，请在 Transition current versions of objects between storage classes (在存储类之间转换对象的当前版本) 下面：

   a. 在 Storage class transitions (存储类转换) 中，选择要过渡到的存储类：

      - Standard-IA (标准 - IA)
      - 智能分层
      - One Zone-IA (单区 - IA)
      - Glacier
      - Glacier Deep Archive (Glacier 深度存档)

   b. 在 Days after object creation (对象创建后的天数) 中，输入创建后转换对象的天数。

   有关存储类的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储类。您可以为当前对象版本和/或之前的对象版本定义转换。版本控制允许您在一个存储桶中保留多个版本的对象。有关版本控制的更多信息，请参阅如何为 S3 存储桶启用或暂停版本控制？ (p. 7)。

   Important

   如果选择 Glacier 或 Glacier Deep Archive 存储类，您的对象将在 Amazon S3 中保留。您无法直接通过单独的 Amazon S3 Glacier 服务访问它们。有关更多信息，请参阅使用 Amazon S3 生命周期转换对象。

8. 要在存储类之间转换对象的非当前版本，请在 Transition non-current versions of objects between storage classes (在存储类之间转换对象的非当前版本) 下面：

   a. 在 Storage class transitions (存储类转换) 中，选择要过渡到的存储类：

      - Standard-IA (标准 - IA)
      - 智能分层
      - One Zone-IA (单区 - IA)
      - Glacier
      - Glacier Deep Archive (Glacier 深度存档)

   b. 在 Days after object becomes non-current (对象成为非当前对象后的天数) 中，输入创建后转换对象的天数。

9. 要使对象的当前版本过期，请在 Expire previous versions of objects (使对象的先前版本过期) 下面的 Number of days after object creation (对象创建后的天数) 中输入天数。

   Important

   在不受版本控制的存储桶中，失效操作会导致 Amazon S3 永久删除该对象。有关生命周期操作的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的描述生命周期操作的元素。

10. 要永久删除对象的先前版本，请在 Permanently delete previous versions of objects (永久删除对象的先前版本) 下面的 Number of days after objects become previous versions (对象成为先前版本后的天数) 中输入天数。
11. 在 Delete expired delete markers or incomplete multipart uploads (删除过期的删除标记或未完成的分段上传) 下面，选择 Delete expired object delete markers (删除过期对象的删除标记) 和 Delete incomplete multipart uploads (删除未完成的分段上传)。然后，输入您要在分段上传启动多少天后结束并清理未完成的分段上传。

    有关分段上传的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的分段上传概述。
12. 选择 Create rule (创建规则)。

    如果规则没有任何错误，Amazon S3 会启用它，并且您可以在 Lifecycle rules (生命周期规则) 下的 Management (管理) 选项卡上看到它。

如何向 S3 存储桶添加复制规则？

复制是在相同或跨不同 AWS 区域中的存储桶自动、异步地复制对象。复制会将源存储桶中新创建的对象和对象更新复制到目标存储桶。有关复制概念以及如何通过 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 使用复制的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制。

复制要求在源存储桶和目标存储桶上均启用了版本控制。要查看要求的完整列表，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制的要求。有关版本控制的更多信息，请参阅如何为 S3 存储桶启用或暂停版本控制？ (p. 7)

目标存储桶中的对象副本是源存储桶中对象的精确副本。它们具有相同的键名和元数据；例如，创建时间、拥有者、用户定义的元数据、版本 ID、访问控制列表 (ACL) 和存储类。您也可以选择为对象副本明确指定不同的存储类。无论谁拥有此源存储桶或源对象，您都可以选择将副本的所有权更改为拥有目标存储桶的 AWS 账户。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的更改副本拥有者。

您可以使用 S3 复制时间控制 (S3 RTC) 在可预测的时间范围内在同一 AWS 区域或跨不同 AWS 区域复制您的数据。S3 RTC 在 15 分钟内复制 Amazon S3 中存储的 99.99% 的新对象，并在几秒钟内复制大多数对象。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 S3 复制时间控制 (S3 RTC) 复制对象。

有关复制和生命周期规则的备注

一个对象的元数据在原始对象和副本对象之间保持相同。生命周期规则遵守原始对象的创建时间，而不是复制的对象在目标存储桶中变为可用状态的时间。但是，在复制完成前，不会对等待复制的对象执行生命周期操作。

您使用 Amazon S3 控制台向源存储桶添加复制规则。复制规则定义要复制的源存储桶对象和存储已复制对象的目标存储桶。您可以创建一条规则，以复制存储桶中的所有对象或具有特定键名前缀和/或一个或多个对象标签的对象子集。目标存储桶与源存储桶可以位于同一 AWS 账户中，也可以位于不同的账户中。

如果您指定要删除的对象版本 ID，Amazon S3 会在源存储桶中删除该对象版本。但不会将删除操作复制到目标存储桶中。换句话说，它不会从目标存储桶中删除同一对象版本。这会防止恶意删除数据。

如果目标存储桶与源存储桶位于不同的账户中，您必须向目标存储桶添加存储桶策略以便为源存储桶账户的所有者授予复制目标存储桶中的对象的权利。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的当源存储桶和目标存储桶由不同的 AWS 账户拥有时授予权限。

当您将复制规则添加到存储桶后，默认情况下将启用复制规则，使该规则在您保存它后立即启动。

主题

- 更多信息 (p. 46)

添加复制规则

当目标存储桶与源存储桶位于同一 AWS 账户中时，可按照以下步骤来配置复制规则。

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择您想要的存储桶的名称。
3. 选择 Management (管理)，向下滚动到 Replication rules (复制规则)，然后选择 Create replication rule (创建复制规则)。
4. 在 Rule name (规则名称) 下，输入规则的名称以帮助稍后标识规则。该名称是必填项，并且它在存储桶内必须是唯一的。
5. 设置 Amazon S3 可以代入以代表您复制对象的 AWS Identity and Access Management (IAM) 角色。

   要设置 IAM 角色，请在 Replication rule configuration (复制规则配置) 部分的 IAM role (IAM 角色) 下，执行以下操作之一：

   - 我们强烈建议您选择 Create new role (创建新角色)，让 Amazon S3 为您创建一个新的 IAM 角色。当您保存该规则后，将为 IAM 角色生成一个与您选择的源和目标存储桶匹配的新策略。生成的角色的名称基于存储桶名称并使用以下命名约定：replication_role_for_***source-bucket***_to_***destination-bucket***。
   - 您可以选择使用现有的 IAM 角色。在这种情况下，您必须选择一个角色，该角色会授予 Amazon S3 必要的权限以进行复制。如果该角色未按照您的复制规则授予 Amazon S3 足够的权限，复制会失败。

     Important

     将复制规则添加到存储桶时，您必须具有 `iam:PassRole` 权限才能传递授予 Amazon S3 复制权限的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的向用户授予将角色传递到 AWS 服务的权限。
6. 在 Status (状态) 下，会看到 Enabled (已启用) 默认处于选中状态。已启用的规则将在您保存它后立即开始工作。如果您想之后启用该规则，请选择 Disabled。
7. 如果存储桶具有现有的复制规则，系统会指示您为规则设置优先级。必须为规则设置优先级，以避免因在多个规则的范围内包含对象而引起冲突。如果规则重叠，Amazon S3 会使用规则优先级确定要应用哪个规则。数字越大，优先级越高。有关规则优先级的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制配置概述。
8. 在 Replication rule configuration (复制规则配置) 中的 Source bucket (源存储桶) 下，您可以通过以下选项设置复制源：

   - 要复制整个存储桶，请选择 This rule applies to all objects in the bucket (此规则将应用于存储桶中的所有对象)。
   - 要复制具有相同前缀的所有对象，请选择 Limit the scope of this rule using one or more filters (使用一个或多个筛选条件限制此规则的范围)。这会将复制限制为名称以字符串 (例如 `pictures`) 开头的所有对象。在框中输入前缀。

     Note

     如果您输入属于文件夹名称的前缀，您必须使用 / (正斜杠) 作为最后一个字符 (例如，`pictures/`)。
   - 要复制具有一个或多个对象标签的所有对象，请选择 Add tag (添加标签)，然后在框中输入键值对。重复上述过程以添加其他标签。您可以组合前缀和标签。有关对象标签的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的对象标签。

新架构支持前缀和标签筛选以及规则的优先级。有关新架构的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制配置向后兼容性。开发人员指南介绍了在用户界面后台工作的 Amazon S3 API 所使用的 XML。在开发人员指南中，将新架构描述为复制配置 XML V2。

9. 在 Destination (目标) 下，您可以使用以下选项来设置复制目标：

   - 要复制到您的账户中的存储桶，请选择 Choose a bucket in this account (选择此账户中的存储桶)，然后键入或浏览目标存储桶。
   - 要复制到其他 AWS 账户中的存储桶，请选择 Choose a bucket in another account (选择另一个账户中的存储桶)，然后输入目标存储桶账户 ID 并键入目标存储桶名称。

     如果目标存储桶与源存储桶位于不同的账户中，您必须向目标存储桶添加存储桶策略以便为源存储桶账户的所有者授予复制目标存储桶中的对象的权利。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的当源存储桶和目标存储桶由不同的 AWS 账户拥有时授予权限。

     Note

     如果未对目标存储桶启用版本控制，您将收到包含 Enable versioning (启用版本控制) 按钮的警告。选择此按钮可对存储桶启用版本控制。

10. 如果要启用 Object Ownership (对象所有权) 以帮助标准化目标存储桶中的新对象的所有权，请选择 Change object ownership to the destination bucket owner (将对象所有权更改为目标存储桶拥有者)。有关此选项的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 S3 RTC 满足合规性要求。

    如果要将数据复制到目标存储桶中的特定存储类，请选择 Change the storage class for the replicated objects (更改已复制对象的存储类)。然后选择要用于目标存储桶中的已复制对象的存储类。如果您不选择此选项，已复制对象的存储类将与原始对象的类相同。

    如果要在复制配置中启用 S3 复制时间控制 (S3 RTC)，请选择 S3 Replication Time Control (S3 复制时间控制)。有关此选项的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 S3 RTC 满足合规性要求。

    Note

    使用 S3 RTC 时，将收取额外的每 GB 数据传输费用和 CloudWatch 指标费用。

11. 要复制源存储桶中使用 AWS Key Management Service (AWS KMS) 加密的对象，请在 Replication criteria (复制标准) 下方，选择 Replicate objects encrypted with AWS KMS (复制使用 AWS KMS 加密的对象)。AWS KMS key for encrypting destination objects (用于加密目标对象的 AWS KMS 密钥) 下是您允许复制使用的源密钥。默认情况下，所有源 CMK 都包含在内。您可以选择缩小 CMK 选择的范围。

    使用您未选择的 AWS KMS CMK 加密的对象不会进行复制。系统为您选择一个 CMK 或一组 CMK，您可以自行选择 CMK。有关将 AWS KMS 用于复制的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制使用具有 AWS KMS 中存储的加密密钥的服务器端加密 (SSE) 创建的对象。

    Important

    在复制使用 AWS KMS 加密的对象时，AWS KMS 请求速率会在源区域中加倍并在目标区域中增加相同的量。之所以对 AWS KMS 的调用率会增加，是因为数据是使用您为复制目标区域定义的客户主密钥 (CMK) 进行重新加密的。对于每个区域的每个调用账户，AWS KMS 设定了一个请求速率限制。有关限制默认值的信息，请参阅《AWS Key Management Service 开发人员指南》中的 AWS KMS 限制 – 每秒请求数：因情况而异。
    如果您在复制期间的当前 Amazon S3 PUT 对象请求速率超过您账户的默认 AWS KMS 速率限制的一半，则建议您请求提高您的 AWS KMS 请求速率限制。要请求提高，请在联系我们处的 AWS Support 中心中创建一个案例。例如，假设您当前的 PUT 对象请求速率为每秒 1000 个请求并且您使用 AWS KMS 加密对象。在此情况下，建议您让 AWS Support 将您在源区域和目标区域（如果不同）中的 AWS KMS 速率限制提高到每秒 2500 个请求，以确保不受 AWS KMS 的限制。

要查看源存储桶中的 PUT 对象请求速率，请查看 Amazon S3 的 Amazon CloudWatch 请求指标中的 `PutRequests`。有关查看 CloudWatch 指标的信息，请参阅如何为 S3 存储桶中的所有对象创建请求指标筛选条件？ (p. 51)

如果您选择复制通过 AWS KMS 加密的对象，请输入 AWS KMS CMK 的 Amazon 资源名称 (ARN)，以便用于加密目标存储桶中的副本。您可以在 IAM 控制台中的 Encryption keys (加密密钥) 下方找到您的 AWS KMS CMK 的 ARN。或者，您可以从下拉列表中选择一个 CMK 名称。

有关创建 AWS KMS CMK 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥。

Important

Amazon S3 控制台只为每个 AWS 区域列出 100 个 AWS KMS CMK。如果您在同一区域中有超过 100 个 CMK，您只会在 S3 控制台中看到前 100 个 CMK。若要使用控制台中未列出的 KMS CMK，请选择自定义 KMS ARN，然后输入相应的 KMS CMK ARN。

12. 要完成，请选择 Save (保存)。
13. 在您保存规则之后，可以通过选择您的规则并选择 Edit rule (编辑规则) 来编辑、启用、禁用或删除您的规则。

授予源存储桶拥有者使用 AWS KMS CMK 加密的权限

您必须向源存储桶拥有者的账户授予权限，以便通过密钥策略使用您的 AWS KMS CMK 进行加密。以下过程介绍如何使用 AWS Identity and Access Management (IAM) 控制台修改 AWS KMS CMK 的密钥策略，该 CMK 用于加密目标存储桶中的副本对象。

授予使用您的 AWS KMS CMK 进行加密的权限

1. 使用拥有该 AWS KMS CMK 的 AWS 账户登录 AWS 管理控制台。从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
2. 选择您在加密时要使用的 CMK 的别名。
3. 在页面的 Key Policy 部分中，选择 Switch to policy view。
4. 选择编辑以编辑密钥策略。
5. 使用 Key Policy (密钥策略) 编辑器，将 Amazon S3 提供的密钥策略插入到现有密钥策略中，然后选择 Save Changes (保存更改)。您可能希望将策略添加到现有策略的末尾。

有关创建和编辑 AWS KMS CMK 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的入门。

更多信息

- 如何管理 S3 存储桶的复制规则？ (p. 46)
- 如何为 S3 存储桶启用或暂停版本控制？ (p. 7)
- 《Amazon Simple Storage Service 开发人员指南》中的复制

如何管理 S3 存储桶的复制规则？

复制是在相同或跨不同 AWS 区域中的存储桶自动、异步地复制对象。它可将源存储桶中新创建的对象和对象更新复制到指定目标存储桶。

您使用 Amazon S3 控制台向源存储桶添加复制规则。复制规则定义了要复制的源存储桶对象和存储复制对象的目标存储桶。有关复制的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制。

您可以在 Replication 页面上管理复制规则。您可以添加、查看、启用、禁用、删除和更改复制规则的优先级。有关向 S3 存储桶添加复制规则的信息，请参阅如何向 S3 存储桶添加复制规则？ (p. 43)。

管理 S3 存储桶的复制规则

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择您想要的存储桶的名称。
3. 选择 Management (管理)，然后向下滚动到 Replication rules (复制规则)。
4. 通过下列方式更改复制规则。
   - 要启用或禁用某个复制规则，请选择该规则，选择 Actions (操作)，然后在下拉列表中，选择 Enable rule (启用规则) 或 Disable rule (禁用规则)。您还可从 Actions (操作) 下拉列表中禁用、启用或删除存储桶中的所有规则。
   - 要更改规则的优先级，请选择规则然后选择 Edit (编辑)，这将启动复制向导以帮助您进行更改。有关使用该向导的信息，请参阅如何向 S3 存储桶添加复制规则？ (p. 43)。

     您需要设置规则优先级，以避免因在多个规则的范围内包含对象而引起冲突。如果规则重叠，Amazon S3 会使用规则优先级确定要应用哪个规则。数字越大，优先级越高。有关规则优先级的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制配置概述。

更多信息

- 如何向 S3 存储桶添加复制规则？ (p. 43)
- 《Amazon Simple Storage Service 开发人员指南》中的复制

如何配置存储类分析？

通过使用 Amazon S3 分析存储类分析工具，您可以分析存储访问模式以帮助您决定何时将正确的数据转换为正确的存储类。存储类分析发现数据访问模式以帮助您确定何时将不常访问的 STANDARD 存储转换为 STANDARD_IA (IA，适用于不常访问) 存储类。有关 STANDARD_IA 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 常见问题和存储类。

> **Important**
>
> 存储类分析不提供转换到 ONEZONE_IA 或 S3 Glacier 存储类的建议。

有关分析的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 分析 – 存储类分析。

配置存储类分析

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其配置存储类分析的存储桶的名称。
3. 选择 Metrics (指标) 选项卡。
4. 在 Storage Class Analysis (存储类分析) 下，选择 Create analytics configuration (创建分析配置)。
5. 为筛选器键入名称。如果要分析整个存储桶，请将 Prefix (前缀) 字段保留为空。
6. 在 Prefix (前缀) 字段中，键入要分析的对象的前缀文本。
7. 要添加标签，请选择添加标签。输入标签的键和值。您可以输入一个前缀和多个标签。
8. （可选）您可以选择 Export CSV (导出 CSV) 下的 Enable (启用) 以将分析报告导出到逗号分隔值 (.csv) 平面文件。选择可将文件存储到的目标存储桶。您可以键入目标存储桶的前缀。目标存储桶必须位于与您为其设置分析的存储桶相同的 AWS 区域中。目标存储桶可处于不同的 AWS 账户中。
9. 选择 Create Configuration (创建配置)。

Amazon S3 在授予 Amazon S3 写入权限的目标存储桶上创建存储桶策略。此操作允许将导出数据写入存储桶中。

Note

此操作将为所有指定的存储桶配置存储类别分析。

如果在您尝试创建存储桶策略出现错误，则将为您提供相关修复说明。例如，如果您在其他 AWS 账户中选择了目标存储桶，而没有权限读取和写入存储桶策略，则您会看到以下消息。您必须让目标存储桶的拥有者将显示的存储桶策略添加到目标存储桶中。如果策略未添加到目标存储桶中，则您不会获得导出数据，因为 Amazon S3 无权写入目标存储桶。如果源存储桶属于其他账户而非当前用户，则在策略中必须替换掉源存储桶的正确账户 ID。

有关导出的数据以及筛选条件的工作原理的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 分析 – 存储类分析。

更多信息

存储管理 (p. 41)

如何配置 Amazon S3 清单？

Amazon S3 清单提供您的对象和元数据的平面文件列表，该列表将有计划地取代 Amazon S3 同步 `List` API 操作。Amazon S3 清单每天或每周为 S3 存储桶或为共享前缀的对象（即，其名称以相同字符串开头的对象）提供逗号分隔值 (CSV) 或 Apache 优化行列式 (ORC) 或 Apache Parquet (Parquet) 输出文件，其中列出您的对象及其对应元数据。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 清单。

配置清单

Note

交付第一份报告可能需要多达 48 小时。

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其配置 Amazon S3 清单的存储桶的名称。
3. 选择 Management (管理)。
4. 在 Inventory configurations (清单配置) 下，选择 Create inventory configuration (创建清单配置)。
5. 在 Inventory configuration name (清单配置名称) 中，输入名称。
6. 设置 Inventory scope (清单范围)：
   - 输入可选的前缀。
   - 选择对象版本：Current versions only (仅限当前版本) 或 Include all versions (包括所有版本)。
7. 在 Report details (报告详细信息) 下，选择要将报告保存到的 AWS 账户的位置：This account (此账户) 或 A different account (另一个账户)。
8. 在 Destination (目标) 下面，选择要将报告保存到的目标存储桶。

   目标存储桶必须位于与您为其设置清单的存储桶相同的 AWS 区域中。目标存储桶可处于不同的 AWS 账户中。在 Destination (目标) 存储桶字段下，您将看到 Destination bucket permission (目标存储桶权限)，该权限添加到目标存储桶策略中以允许 Amazon S3 在该存储桶中放置数据。有关更多信息，请参阅目标存储桶策略 (p. 50)。
9. 在 Frequency (频率) 下，选择生成报告的频率：Daily (每日) 或 Weekly (每周)。
10. 选择报告的 Output format (输出格式)：

- CSV
- Apache ORC
- Apache Parquet

11. 在 Status (状态) 下，选择 Enable (启用) 或 Disable (禁用)。
12. 要使用服务器端加密，请在 Server-side encryption (服务器端加密) 下，执行以下步骤：

    a. 选择启用。

    b. 在 Encryption key type (加密密钥类型) 下，选择 Amazon S3 key (SSE-S3) (Amazon S3 密钥 (SSE-S3)) 或 AWS Key Management Service key (SSE-KMS) (AWS Key Management Service 密钥 (SSE-KMS))。

    Amazon S3 服务器端加密使用 256 位高级加密标准 (AES-256)。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 托管加密密钥 (SSE-S3)。有关 SSE-KMS 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 AWS KMS CMK。

    c. 要使用 AWS KMS CMK，请选择以下选项之一：

    - AWS managed key (aws/s3) (AWS 托管密钥 (aws/S3))
    - Choose from your KMS master keys (从您的 KMS 主密钥中选择)，然后选择 KMS master key (KMS 主密钥)。
    - Enter KMS master key ARN (输入 KMS 主密钥 ARN)，然后输入您的 AWS KMS 密钥 ARN。

    Note

    要使用 SSE-KMS 加密清单列表文件，您必须授予 Amazon S3 使用 AWS KMS CMK 的权限。有关说明，请参阅授予 Amazon S3 使用 AWS KMS CMK 进行加密的权限 (p. 50)。

13. 对于 Additional fields (其他字段)，从下面选择一项或多项以添加到清单报告：

    - Size (大小) – 对象大小（以字节为单位）。
    - Last modified date (上次修改日期) – 对象创建日期或上次修改日期（以较晚者为准）。
    - Storage class (存储类) – 用于存储对象的存储类。
    - ETag (实体标签) – 实体标签是对象的哈希。ETag 仅反映对对象内容的更改，而不反映对其元数据的更改。ETag 可能是也可能不是对象数据的 MD5 摘要。是与不是取决于对象的创建方式和加密方式。
    - Multipart upload (分段上传) – 指定对象以分段上传形式上传。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的分段上传概述。
    - Replication status (复制状态) – 对象的复制状态。有关更多信息，请参阅如何向 S3 存储桶添加复制规则？ (p. 43)。
    - Encryption status (加密状态) – 用于加密对象的服务器端加密。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用服务器端加密保护数据。
    - Object lock configurations (对象锁定配置) – 对象的对象锁定状态，包括以下设置：
      - Retention mode (保留模式) – 应用于对象的保护级别，可以是 Governance (监管)或 Compliance (合规)。
      - Retain until date (保留到期日期) – 在此日期之前无法删除锁定对象。
      - Legal hold status (依法保留状态) – 锁定对象的依法保留状态。

    有关 S3 对象锁定的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 S3 对象锁定概述。

有关清单报告内容的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 清单中包含了什么？。

14. 选择创建。

目标存储桶策略

Amazon S3 在授予 Amazon S3 写入权限的目标存储桶上创建存储桶策略。这样，Amazon S3 就能够将清单报告的数据写入存储桶。

如果在您尝试创建存储桶策略出现错误，则将为您提供相关修复说明。例如，如果您在其他 AWS 账户中选择了目标存储桶，而没有权限读取和写入存储桶策略，则您会看到一条错误消息。

在这种情况下，目标存储桶拥有者必须将显示的存储桶策略添加到目标存储桶中。如果策略未添加到目标存储桶中，则您不会获得清单报告，因为 Amazon S3 无权写入目标存储桶。如果源存储桶属于其他账户而非当前用户，则在策略中必须替换掉源存储桶的正确账户 ID。

有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 清单。

向 Amazon S3 授予权限以使用 AWS KMS CMK 进行加密

要向 Amazon S3 授予使用客户托管 AWS Key Management Service (AWS KMS) 客户主密钥 (CMK) 进行加密的权限，必须使用密钥策略。要更新密钥策略，以便您能够使用 AWS KMS 客户托管 CMK 加密清单文件，请按照以下步骤操作。

授予使用您的 AWS KMS CMK 进行加密的权限

1. 使用拥有客户托管 CMK 的 AWS 账户，登录 AWS 管理控制台。
2. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
3. 要更改 AWS 区域，请使用页面右上角的区域选择器。
4. 在左侧导航窗格中，选择 Customer managed keys (客户托管密钥)。
5. 在 Customer managed keys (客户托管密钥) 下，选择要用于加密清单文件的客户托管 CMK。
6. 在 Key policy (密钥策略) 下，选择 Switch to policy view (切换到策略视图)。
7. 要更新密钥策略，请选择 Edit (编辑)。
8. 在 Edit key policy (编辑密钥策略) 下，将以下密钥策略添加到现有密钥策略。

```
{
    "Sid": "Allow Amazon S3 use of the CMK",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

9. 选择保存更改。

   有关创建 AWS KMS 客户托管 CMK 和使用密钥策略的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的以下链接：

   - 入门
   - 在 AWS KMS 中使用密钥策略

更多信息

存储管理 (p. 41)

如何为 S3 存储桶中的所有对象创建请求指标筛选条件？

Amazon S3 存在三种类型的 Amazon CloudWatch 指标：存储指标、请求指标和复制指标。存储指标每天报告一次并提供给所有客户，无需额外费用。请求指标在要处理的某些延迟后每隔一分钟提供一次。请求指标按标准 CloudWatch 费率计费。您必须通过在控制台中配置请求指标或使用 Amazon S3 API 来选择使用请求指标。

有关 Amazon S3 的 CloudWatch 指标的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon CloudWatch 监控指标。

创建请求指标筛选器

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，选择您要为其获取请求指标的对象所在的存储桶的名称。
3. 选择 Metrics (指标) 选项卡。
4. 在 Bucket metrics (存储桶指标) 下，选择 View additional charts (查看其他图表)。
5. 选择 Request metrics (请求指标) 选项卡。
6. 选择 Create filter (创建筛选器)。
7. 在 Filter name (筛选器名称) 框中，输入筛选器名称。

   名称可以包含字母、数字、句点、短划线和下划线。建议对应用于所有对象的筛选器使用 `EntireBucket` 作为名称。
8. 在 Choose a filter scope (选择筛选范围) 下，选择 This filter applies to all objects in the bucket (此筛选器将应用于存储桶中的所有对象)。

   您还可以定义筛选器，以便仅对此存储桶中的一部分对象收集和报告指标。有关更多信息，请参阅 如何创建通过对象标签或前缀限制范围的请求指标筛选条件？ (p. 51)。
9. 选择 Create filter (创建筛选器)。
10. 在 Request metrics (请求指标) 选项卡的 Filters (筛选器) 下，选择刚创建的筛选器。

    大约 15 分钟后，CloudWatch 开始跟踪这些请求指标。您可以在 Request metrics (请求指标) 选项卡上查看它们。您可以在 Amazon S3 或 CloudWatch 控制台上查看指标的图形。请求指标按标准 CloudWatch 费率计费。有关更多信息，请参阅 Amazon CloudWatch 定价。

如何创建通过对象标签或前缀限制范围的请求指标筛选条件？

Amazon S3 存在三种类型的 Amazon CloudWatch 指标：存储指标、请求指标和复制指标。存储指标每天报告一次并提供给所有客户，无需额外费用。请求指标在要处理的某些延迟后每隔一分钟提供一次。请求指标按标准 CloudWatch 费率计费。您必须通过在控制台中配置请求指标或使用 Amazon S3 API 来选择使用请求指标。

有关 Amazon S3 的 CloudWatch 指标的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon CloudWatch 监控指标。

为存储桶中的一部分对象筛选请求指标

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，选择您要为其获取请求指标的对象所在的存储桶的名称。
3. 选择 Metrics (指标) 选项卡。
4. 在 Bucket metrics (存储桶指标) 下，选择 View additional charts (查看其他图表)。
5. 选择 Request metrics (请求指标) 选项卡。
6. 选择 Create filter (创建筛选器)。
7. 在 Filter name (筛选器名称) 框中，输入筛选器名称。

   名称可以包含字母、数字、句点、短划线和下划线。
8. 在 Choose a filter scope (选择筛选范围) 下，选择 Limit the scope of this filter using prefix and tags (使用前缀和标签限制此筛选器的范围)。
9. （可选）在 Prefix (前缀) 框中，输入前缀以将筛选器的范围限制为单个路径。
10. （可选）在 Tags (标签) 下，输入标签 Key (键) 和 Value (值)。
11. 选择 Create filter (创建筛选器)。

    Amazon S3 会创建使用您指定的标签或前缀的筛选器。
12. 在 Request metrics (请求指标) 选项卡的 Filters (筛选器) 下，选择刚创建的筛选器。

    您现在已创建一个筛选条件，该筛选条件通过对象标签和前缀限制请求指标范围。在 CloudWatch 开始跟踪这些请求指标后大约 15 分钟，您就可以看到 Amazon S3 和 CloudWatch 控制台中的指标的图表。请求指标按标准 CloudWatch 费率计费。有关更多信息，请参阅 Amazon CloudWatch 定价。

    还可以在存储桶级别配置请求指标。想要了解有关信息，请参阅 如何为 S3 存储桶中的所有对象创建请求指标筛选条件？ (p. 51)

如何删除请求指标筛选条件？

在 Amazon S3 控制台中，您可以删除请求指标筛选条件。删除筛选条件时，您不再需要为使用该特定筛选条件 的请求指标付费。但是，您将继续为存在的任何其他筛选条件配置付费。删除筛选条件时，您不再能够对请求指标使用筛选条件。删除筛选条件的操作无法撤消。

有关创建请求指标筛选条件的更多信息，请参阅如何为 S3 存储桶中的所有对象创建请求指标筛选条件？ (p. 51)和如何创建通过对象标签或前缀限制范围的请求指标筛选条件？ (p. 51)

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket (存储桶) 列表中，选择您的存储桶名称。
3. 选择 Metrics (指标) 选项卡。
4. 在 Bucket metrics (存储桶指标) 下，选择 View additional charts (查看其他图表)。
5. 选择 Request metrics (请求指标) 选项卡。
6. 选择 Manage filters (管理筛选条件)。
7. 选择您的筛选条件。

   Important

   删除筛选条件的操作无法撤消。
8. 选择 Delete。

   Amazon S3 会删除您的筛选条件。

如何查看复制指标？

Amazon S3 存在三种类型的 Amazon CloudWatch 指标：存储指标、请求指标和复制指标。当您通过 AWS 管理控制台或 Amazon S3 API 使用 S3 复制时间控制 (S3 RTC) 启用复制时，复制指标将自动打开。使用 S3 复制时间控制 (S3 RTC) 启用复制规则后 15 分钟即可使用复制指标。

复制指标跟踪复制配置的规则 ID。复制规则 ID 可以特定于前缀、标签或两者的组合。有关 S3 复制时间控制 (S3 RTC) 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 S3 复制时间控制 (S3 RTC) 复制对象。

有关 Amazon S3 的 CloudWatch 指标的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon CloudWatch 监控指标。

先决条件

启用具有 S3 RTC 的复制规则。

查看复制指标

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择您要为其获取复制指标的对象所在的存储桶的名称。
3. 选择 Metrics (指标) 选项卡。
4. 在 Replication metrics (复制指标) 下，选择 Replication rules (复制规则)。
5. 选择 Display charts (显示图表)。

   Amazon S3 将在图表中显示 Replication Latency (in seconds) [复制延迟（以秒为单位）]、Operations pending replication (待复制的操作)。
6. 要在单独的页面上一起查看所有复制指标，包括 Bytes pending replication (待复制的字节数)、Replication Latency (in seconds) [复制延迟（以秒为单位）] 和 Operations pending replication (待复制的操作)，请选择 View 1 more chart (再查看 1 张图表)。

然后，您可以查看所选规则的复制指标 Replication Latency (in seconds) [复制延迟（以秒为单位）]、Operations pending replication (待复制的操作) 和 Bytes pending replication (待复制的字节数)。Amazon CloudWatch 在相应的复制规则上启用 S3 RTC 后 15 分钟开始报告复制指标。您可以在 Amazon S3 或 CloudWatch 控制台上查看复制指标。有关信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的复制指标概述。

设置存储桶和对象访问权限

本部分介绍如何使用 Amazon Simple Storage Service (Amazon S3) 控制台授予存储桶和对象的访问权限。本部分还介绍如何使用 Amazon S3 阻止公有访问来阻止使用允许对 S3 存储桶中的数据进行公有访问的任何设置的应用程序。

存储桶和对象是 Amazon S3 资源。您使用基于资源的访问策略来授予对存储桶和对象的访问权限。您可以将访问策略与资源关联。访问策略描述了谁可以访问资源。资源所有者是创建资源的 AWS 账户。有关资源所有权和访问策略的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的有关管理访问的概述。

存储桶访问权限 指定了拥有对存储桶中的对象的访问权限的用户以及他们拥有的访问权限的类型。对象访问权限 指定了拥有对象访问权限的用户以及他们拥有的访问权限的类型。例如，一个用户可能只有读取权限，而另一个人可能有读写权限。

存储桶和对象的权限是相互独立的。对象不继承其存储桶的权限。例如，如果您创建了一个存储桶并授予一个用户写入权限，则将无法访问此用户的对象，除非此用户显式授予您访问权限。利用存储桶权限，用户通常可以列出有关存储桶的信息，并在存储桶中添加和删除对象。利用对象权限，用户通常可以下载、替换或删除对象。

> **Note**
>
> 要授予对象权限，您不一定需要授予存储桶权限，反之亦然。例如，您可以使用 AWS 控制台向用户授予对某个对象的更新权限，而不向此用户授予对包含该对象的存储桶的权限。但是，如果您只授予对象权限，而不授予存储桶权限，则被授权者将无法使用 AWS 控制台访问对象。（由于他们无法查看包含对象的存储桶，因此无法在控制台中查看对象。）被授权者必须改为以编程方式访问对象，例如使用 AWS CLI。

要向其他 AWS 账户和公众授予对存储桶和对象的访问权限，可使用称为访问控制列表 (ACL) 的基于资源的访问策略。

存储桶策略是一种基于资源的 AWS Identity and Access Management (IAM) 策略，可向其他 AWS 账户或 IAM 用户授予对 S3 存储桶的访问权限。存储桶策略补充 (在很多情况下取代) 基于 ACL 的访问策略。有关将 IAM 与 Amazon S3 结合使用的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的管理对 Amazon S3 资源的访问权限。

有关管理访问权限的更多深入信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 资源访问权限管理介绍。

本节还说明如何使用 Amazon S3 控制台向 S3 存储桶添加跨源资源共享 (CORS) 配置。CORS 允许在一个域中加载的客户端 Web 应用程序与另一个域中的资源进行交互。

主题

- 使用 S3 访问分析器 (p. 61)

如何对 S3 存储桶阻止公有访问？

Amazon S3 阻止公有访问将阻止使用允许对 S3 存储桶中的数据进行公有访问的任何设置的应用程序。您可以为单个 S3 存储桶或账户中的所有存储桶配置阻止公有访问设置。有关使用 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 阻止公有访问的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 阻止公有访问。

以下主题介绍如何使用 Amazon S3 控制台配置阻止公有访问设置：

- 如何为 S3 存储桶编辑公有访问设置？ (p. 55)
- 如何为 AWS 账户中的所有 S3 存储桶编辑公有访问设置？ (p. 56)

下面几节介绍查看存储桶访问状态和按访问类型进行搜索。

查看访问状态

“List buckets (列出存储桶)”视图显示您的存储桶是否可公开访问。Amazon S3 会标注存储桶的权限，如下所示：

- 公有 – 所有人都拥有以下一项或多项访问权限：列出对象、写入对象、读取和写入权限。
- 对象可以是公有的 – 存储桶不是公有的，但具有适当权限的任何人都可以授予对象公有访问权限。
- 存储桶和对象不是公有的 – 存储桶和对象没有任何公有访问权限。
- 仅限此账户的授权用户 – 由于存在授予公有访问权限的策略，因此访问权限仅限于此账户中的 IAM 用户和角色以及 AWS 服务委托人。

访问列显示列出的存储桶的访问状态。

您还可以按访问类型来筛选存储桶搜索。从 Search for bucket (搜索存储桶) 栏旁边的下拉列表中选择一种访问类型。

更多信息

- 如何为 S3 存储桶编辑公有访问设置？ (p. 55)
- 如何为 AWS 账户中的所有 S3 存储桶编辑公有访问设置？ (p. 56)
- 设置存储桶和对象访问权限 (p. 54)
- 《Amazon Simple Storage Service 开发人员指南》中的使用源访问身份限制访问
- AWS 开发人员博客中的访问 Amazon CloudFront 中的私有内容

如何为 S3 存储桶编辑公有访问设置？

Amazon S3 阻止公有访问将阻止使用允许对 S3 存储桶中的数据进行公有访问的任何设置的应用程序。本部分介绍如何为一个或多个 S3 存储桶编辑阻止公有访问设置。有关使用 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 阻止公有访问的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 阻止公有访问。

主题

- 为 S3 存储桶编辑公有访问设置 (p. 56)

- 更多信息 (p. 56)

为 S3 存储桶编辑公有访问设置

如何您需要为单个 S3 存储桶更改公有访问设置，请执行以下步骤。

为 S3 存储桶编辑 Amazon S3 阻止公有访问设置

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择您想要的存储桶的名称。
3. 选择权限。
4. 选择 Edit (编辑) 以更改存储桶的公有访问设置。有关四个 Amazon S3 阻止公有访问设置的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的阻止公有访问设置。
5. 选择要更改的设置，然后选择 Save changes (保存更改)。
6. 当系统要求确认时，请输入 **`confirm`**。然后选择 Confirm (确认) 以保存更改。

在创建存储桶时，可以更改 Amazon S3 阻止公有访问设置。有关更多信息，请参阅 如何创建 S3 存储桶？ (p. 3)。

更多信息

- 如何对 S3 存储桶阻止公有访问？ (p. 55)
- 如何为 AWS 账户中的所有 S3 存储桶编辑公有访问设置？ (p. 56)
- 设置存储桶和对象访问权限 (p. 54)

如何为 AWS 账户中的所有 S3 存储桶编辑公有访问设置？

Amazon S3 阻止公有访问将阻止所有在设置中允许对 S3 存储桶中的数据进行公有访问的应用程序。本部分介绍如何为 AWS 账户中的所有 S3 存储桶编辑阻止公有访问设置。有关使用 AWS CLI、AWS 开发工具包和 Amazon S3 REST API 阻止公有访问的信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 阻止公有访问。

为 AWS 账户中的所有 S3 存储桶编辑阻止公有访问设置

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 选择 Account settings for Block Public Access (账户的阻止公有访问设置)。
3. 选择 Edit (编辑) 以便为 AWS 账户中的所有存储桶更改阻止公有访问设置。
4. 选择要更改的设置，然后选择 Save changes (保存更改)。
5. 当系统要求确认时，请输入 **`confirm`**。然后选择 Confirm (确认) 以保存更改。

更多信息

- 如何对 S3 存储桶阻止公有访问？ (p. 55)
- 如何为 S3 存储桶编辑公有访问设置？ (p. 55)

- 设置存储桶和对象访问权限 (p. 54)

如何在对象上设置权限？

本节介绍如何使用 Amazon Simple Storage Service (Amazon S3) 控制台通过访问控制列表 (ACL) 管理 Amazon S3 对象的访问权。ACL 是基于资源的访问策略，可授予对存储桶和对象的访问权。有关使用基于资源的策略管理访问权的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的有关管理访问的概述。

存储桶和对象的权限是相互独立的。对象不继承其存储桶的权限。例如，如果您创建了一个存储桶并授予一个用户写入权限，则将无法访问此用户的对象，除非此用户显式授予您访问权限。

您可以向其他 AWS 账户或预定义的组授予权限。您向其授予权限的用户或组称作被授权者。默认情况下，所有者 (即创建存储桶的 AWS 账户) 具有完全权限。

您为用户或组授予的每项权限都会在 ACL 中添加一个与该对象关联的条目。ACL 列出了授权，这些授权确定了被授权者和授予的权限。有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 ACL 管理访问权限。

为对象设置权限

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择包含要为其设置权限的对象的存储桶的名称。
3. 选择 Bucket overview (存储桶概述) 部分下的选项卡列表中显示的 Permissions (权限) 选项卡。
4. 要编辑阻止公有访问设置，请选择 Edit (编辑) 以阻止或允许对此存储桶及其访问点的公有访问。有关更多信息，请参阅阻止公有访问 (p. 55)。
5. 要编辑存储桶策略，请选择 Edit (编辑) 以编辑提供对此存储桶中存储的对象的访问权限的 JSON 存储桶策略。此策略仅适用于您的账户拥有的对象。

   或者，如果您有现有的存储桶策略，则可以选择 Delete (删除) 来删除现有的存储桶策略。有关更多信息，请参阅添加存储桶策略 (p. 59)。
6. 要编辑对象所有权，请选择 Edit (编辑) 以取得上传到此存储桶的新对象的所有权。有关更多信息，请参阅??? (p. 61)。
7. 要编辑访问控制列表 (ACL)，请选择 Edit (编辑) 以更新被授予者组（例如存储桶拥有者（您的 AWS 账户）、所有人、已验证身份用户（拥有 AWS 账户的任何人）或 S3 日志传输组）的权限（列出、读取和写入）。

   a. 存储桶拥有者 是指您的 AWS 账户，而不是 AWS Identity and Access Management (IAM) 用户。有关根用户的更多信息，请参阅《IAM 用户指南》中的 AWS 账户根用户。
   b. 要将对象的访问权限授予所有人，请选择 Everyone (所有人)。授予公有访问权限意味着世界上的任何人都可以访问该对象。

      Warning

      - 在授予 Everyone (所有人) 组对您的 Amazon S3 对象的匿名访问权限时应谨慎使用。如果您向此组授予访问权限，那么世界上的任何人都可以访问您的对象。如果您需要为所有人授予访问权限，我们强烈建议您仅授予读取对象的权限。
      - 我们强烈建议您不要为 Everyone 组授予写入对象权限。这样做将允许任何人覆盖对象的 ACL 权限。

   c. 要向其他 AWS 账户中的 AWS 用户授予权限，请输入要向其授予对象权限的 AWS 用户的规范 ID。有关查找规范 ID 的信息，请参阅《Amazon Web Services 一般参考》中的 AWS 账户标识符。您可以添加多达 99 个用户。
   d. 要指定 S3 日志传输组，请提供您希望 Amazon S3 在其中将访问日志保存为对象的目标存储桶的名称。

有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的设置 ACL 存储桶权限 (p. 58)和如何启用服务器访问日志记录。

8. 要编辑跨源资源共享 (CORS)，请选择 Edit (编辑) 以创建 CORS 配置，该配置是一个 XML 文档，用于定义在一个域中加载的客户端 Web 应用程序如何与其他域中的资源进行交互。有关更多信息，请参阅通过 CORS 添加跨域资源共享 (p. 60)。
9. 在前面的步骤中编辑任何设置之后，在完成时选择 Save changes (保存更改)。

   Note

   此操作将权限应用于所有指定的对象。将权限应用到文件夹时，请等待保存操作完成，然后再添加新对象。

您也可以在上传对象时设置对象权限。有关在上传对象时设置权限的更多信息，请参阅上传 S3 对象 (p. 22)。

更多信息

- 设置存储桶和对象访问权限 (p. 54)
- 如何设置 ACL 存储桶权限？ (p. 58)

如何设置 ACL 存储桶权限？

本节介绍如何使用 Amazon Simple Storage Service (Amazon S3) 控制台通过访问控制列表 (ACL) 管理 S3 存储桶的访问权限。ACL 是基于资源的访问策略，可授予对存储桶和对象的访问权。有关使用基于资源的策略管理访问权的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的有关管理访问的概述。

您可以向其他 AWS 账户用户或预定义的组授予权限。您将向其授予权限的用户或组称作被授权者。默认情况下，所有者 (即创建存储桶的 AWS 账户) 具有完全权限。

您为用户或组授予的每项权限都会在 ACL 中添加一个与该存储桶关联的条目。ACL 列出了授权，这些授权确定了被授权者和授予的权限。有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 ACL 管理访问权限。

Warning

我们强烈建议您避免向所有人（公有访问）或经过身份验证的用户组（所有经 AWS 身份验证的用户）群组授予写入访问权限。有关向这些组授予写访问权限所产生影响的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的 Amazon S3 预定义组。

设置 S3 存储桶的 ACL 访问权限

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其配置权限的存储桶的名称。
3. 选择 Permissions (权限)，然后选择 Access Control List (ACL) (访问控制列表) 内的 Edit (编辑)。
4. 您可以管理存储桶的以下访问权限：

   a. AWS 账户根用户的访问权限

      owner (拥有者) 是指 AWS 账户根用户，而不是 AWS Identity and Access Management (IAM) 用户。有关根用户的更多信息，请参阅《IAM 用户指南》中的 AWS 账户根用户。

要更改所有者的存储桶访问权限，请选中 Bucket owner (your AWS account) (存储桶拥有者（您的 AWS 账户）) 下的权限复选框。

b. 其他 AWS 账户的访问权限

要向其他 AWS 账户中的 AWS 用户授予权限，请选择 Add grantee (添加被授权者)。在 Enter a canonical ID (输入规范 ID) 字段中，输入要向其授予存储桶权限的 AWS 用户的规范 ID 或电子邮件。有关查找规范 ID 的信息，请参阅《Amazon Web Services 一般参考》中的 AWS 账户标识符。您可以添加多达 99 个用户。

选中要向用户授予的权限旁边的复选框，然后选择 Save changes (保存更改)。

Warning

当您需要向其他 AWS 账户授权访问您的资源时，注意 AWS 账户可以向其账户下的用户授予权限。这称为跨账户访问。有关使用跨账户访问的信息，请参阅《IAM 用户指南》中的创建角色以向 IAM 用户委派权限。

c. 公有访问权限

要向一般公众 (世界上的每一个人) 授予对您的存储桶的访问权限，请在 Public access 下面选择 Everyone。授予公有访问权限意味着世界上的任何人都可以访问该存储桶。选中要授予的权限所对应的复选框，然后选择 Save。

要撤消授予对您的存储桶的公共访问权限，请在 Public access (公有访问权限) 下面选择 Everyone (任何人)。清除所有权限复选框，然后选择 Save (保存)。

Warning

在授予 Everyone 组对您的 S3 存储桶的公有访问权限时应谨慎使用。如果您向此组授予访问权限，那么世界上的任何人都可以访问您的存储桶。我们强烈建议您绝对不要授予对 S3 存储桶的任何类型的公有写入权限。

d. S3 日志传输组

要授予对 Amazon S3 的访问权限以便将服务器访问日志写入存储桶，请在 S3 log delivery group (S3 日志传输组) 下面选择 Log Delivery (日志传输)。

如果存储桶设置为目标存储桶以接收访问日志，则存储桶权限必须允许日志传输组对存储桶有写入权限。当您在存储桶上启用服务器访问日志记录时，Amazon S3 控制台会向 Log Delivery (日志传输) 组授予对您选择用来接收日志的目标存储桶的写入权限。有关服务器访问日志记录的更多信息，请参阅如何为 S3 存储桶启用服务器访问日志记录？ (p. 8)。

您还可以在创建存储桶时设置存储桶权限。有关在创建存储桶时设置权限的更多信息，请参阅如何创建 S3 存储桶？ (p. 3)。

更多信息

- 设置存储桶和对象访问权限 (p. 54)
- 如何在对象上设置权限？ (p. 57)
- 如何添加 S3 存储桶策略？ (p. 59)

如何添加 S3 存储桶策略？

本节说明如何使用 Amazon Simple Storage Service (Amazon S3) 控制台添加新存储桶策略或编辑现有存储桶策略。存储桶策略是基于资源的 AWS Identity and Access Management (IAM) 策略。将存储桶策略添加到一个存储桶可向其他 AWS 账户或 IAM 用户授予对该存储桶以及其中对象的访问权限。对象权限仅应用于存

储桶拥有者创建的对象。有关存储桶策略的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的有关管理访问的概述。

有关 Amazon S3 存储桶策略的示例，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储桶策略示例。

创建或编辑存储桶策略

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其创建或编辑存储桶策略的存储桶的名称。
3. 选择 Permissions。
4. （可选）选择 Policy generator (策略生成器) 以在新窗口中打开 AWS Policy Generator。在策略生成器页面上，从 Select Type of Policy (选择策略类型) 下拉菜单中选择 S3 Bucket Policy (S3 存储桶策略)。通过填充显示的字段来添加一个或多个语句，然后选择 Generate Policy (生成策略)。复制生成的策略文本，然后返回到 Amazon S3 控制台中的 Edit bucket policy (编辑存储桶策略) 页面。
5. 在 Bucket policy (存储桶策略) 下，选择 Edit (编辑)。
6. 在 Policy (策略) 文本字段中，键入或复制并粘贴新的存储桶策略，或者编辑现有策略。存储桶策略是一个 JSON 文件。您在编辑器中键入的文本必须是有效的 JSON。

   Note

   为方便起见，控制台会在 Policy (策略) 文本字段上方显示当前存储桶的 Amazon 资源名称 (ARN)。您可以复制此 ARN 以便在策略中使用。有关 ARN 的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 资源名称 (ARN) 和 AWS 服务命名空间。
7. 选择 Save。

更多信息

- 设置存储桶和对象访问权限 (p. 54)
- 如何设置 ACL 存储桶权限？ (p. 58)

如何通过 CORS 添加跨域资源共享？

本节说明如何使用 Amazon S3 控制台向 S3 存储桶添加跨源资源共享 (CORS) 配置。CORS 允许在一个域中加载的客户端 Web 应用程序与另一个域中的资源进行交互。

要将您的存储桶配置为允许跨源请求，您可以将 CORS 配置添加到存储桶。CORS 配置是一个定义规则的文档，这些规则标识可访问您的存储桶的源、每个源支持的操作 (HTTP 方法) 以及其他操作特定的信息。在 S3 控制台中，CORS 配置必须是 JSON 文档。有关 CORS 及示例的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的跨源资源共享 (CORS)。

在存储桶上启用 CORS 时，访问控制列表 (ACL) 和其他访问权限策略仍适用。

Important

在新的 S3 控制台中，CORS 配置必须是 JSON。

将 CORS 配置添加到 S3 存储桶

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其创建存储桶策略的存储桶的名称。
3. 选择 Permissions。

4. 在 Cross-origin resource sharing (CORS) (跨源资源共享 (CORS)) 部分中，选择 Edit (编辑)。
5. 在 Cross-origin resource sharing (CORS) (跨源资源共享 (CORS)) 文本框中，键入或复制并粘贴新的 CORS 配置，或者编辑现有配置。

   在 S3 控制台中，CORS 配置是 JSON 文件。您在编辑器中键入的文本必须是有效的 JSON。有关更多信息及示例，请参阅如何在我的存储桶上配置 CORS？
6. 选择保存更改。

   Note

   Amazon S3 在 CORS configuration editor 标题旁边显示存储桶的 Amazon 资源名称 (ARN)。有关 ARN 的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 资源名称 (ARN) 和 AWS 服务命名空间。

更多信息

- 设置存储桶和对象访问权限 (p. 54)
- 如何设置 ACL 存储桶权限？ (p. 58)
- 如何添加 S3 存储桶策略？ (p. 59)

在 AWS 管理控制台中将 S3 对象所有权设置为首选的存储桶拥有者

S3 对象所有权目前处于预览状态，可以通过 AWS 管理控制台、AWS 命令行界面、AWS 开发工具包或 Amazon S3 REST API 进行配置。计划正式发布 AWS CloudFormation 支持。

S3 对象所有权使您能够获得其他 AWS 账户使用 `bucket-owner-full-control` 标准访问控制列表 (ACL) 上传到存储桶的新对象的所有权。本节介绍如何使用控制台设置对象所有权。

在 S3 存储桶上将对象所有权设置为首选的存储桶拥有者

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要为其启用 S3 对象所有权的存储桶的名称。
3. 选择 Permissions 选项卡。
4. 选择 Object Ownership (对象所有权) 下的 Edit (编辑)。
5. 选择首选的存储桶拥有者，然后选择保存。

如何确保我拥有新对象的所有权？

通过上述步骤，对象所有权将取得由其他账户使用 `bucket-owner-full-control` 标准 ACL 写入的任何新对象的所有权。有关强制实施对象所有权的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的如何确保我拥有新对象的所有权？。

使用 S3 访问分析器

如果存在已配置为允许 Internet 上的任何人或其他 AWS 账户（包括组织外部的 AWS 账户）访问的 S3 存储桶，S3 访问分析器会向您发出提醒。对于每个公共存储桶或共享存储桶，您会收到有关公共或共享访问的来

源和级别的信息。例如，S3 访问分析器可能会显示存储桶具有通过存储桶访问控制列表 (ACL)、存储桶策略或访问点策略提供的读取或写入访问权限。掌握了这些信息，您就可以立即采取精确的纠正措施，将存储桶访问权限恢复为您期望的设置。

在 S3 访问分析器中查看存在风险的存储桶时，只需单击一下即可阻止对存储桶的所有公有访问。我们建议您阻止所有对存储桶的访问，除非您需要公有访问才能支持特定使用案例。在阻止所有公有访问之前，请确保您的应用程序在没有公有访问权限的情况下可以继续正常工作。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 阻止公有访问。

您还可以向下钻取到存储桶级别权限设置，以配置精细访问。对于需要公有访问的特定和经验证的使用案例（例如静态网站托管、公共下载或跨账户共享），您可以通过对存储桶的结果进行存档来确认和记录存储桶保持公开或共享的意图。您可以随时重新访问和修改这些存储桶配置。您还可以将结果下载为 CSV 格式的报告以供审计使用。

Amazon S3 控制台上提供 S3 访问分析器，无需额外费用。S3 访问分析器由 AWS Identity and Access Management (IAM) 访问分析器提供支持。要在 Amazon S3 控制台上使用 S3 访问分析器，您必须访问 IAM 控制台，然后按区域启用 IAM 访问分析器。

有关 IAM 访问分析器的更多信息，请参阅《IAM 用户指南》中的什么是访问分析器？有关 S3 访问分析器的更多信息，请查看以下部分。

Important

- S3 访问分析器需要账户级分析器。要使用 S3 访问分析器，您必须访问 IAM 访问分析器并创建具有一个账户作为信任区域的分析器。有关更多信息，请参阅《IAM 用户指南》中的启用访问分析器。
- 添加或修改存储桶策略或存储桶 ACL 后，访问分析器会在 30 分钟内根据更改生成和更新结果。与账户级别阻止公有访问设置相关的结果可能在您更改设置后长达 6 小时无法生成或更新。

主题

S3 访问分析器提供哪些信息？

S3 访问分析器提供可在 AWS 账户之外访问的存储桶的结果。Internet 上的任何人均可访问在 Buckets with public access (具有公有访问权限的存储桶) 下面列出的存储桶。如果 S3 访问分析器标识了公有存储桶，您还会在页面顶部看到一条警告，其中显示您的区域中公有存储桶的数量。Buckets with access from other AWS accounts — including third-party AWS accounts (可从其他 AWS 账户（包括第三方 AWS 账户）访问的存储桶) 下面列出的存储桶将与其他 AWS 账户（包括组织外部的账户）有条件地共享。

对于每个存储桶，S3 访问分析器提供以下信息：

- Bucket name
- Discovered by Access analyzer (由访问分析器发现) - 当 S3 访问分析器发现公有或共享存储桶访问时。
- Shared through (共享方式) - 如何通过存储桶策略、存储桶 ACL 或访问点策略共享存储桶。可以通过策略和 ACL 来共享存储桶。如果您想要找到并查看存储桶访问的来源，您可以使用此列中的信息作为起点，立即采取精确的纠正措施。

- Status (状态) - 存储桶结果的状态。S3 访问分析器显示所有公有存储桶和共享存储桶的结果。
  - Active (活动) - 结果尚未审核。
  - Archived (已存档) - 结果已按预期审核和确认。
  - All (全部) - 公有存储桶或与其他 AWS 账户（包括组织外部的 AWS 账户）共享的存储桶的所有结果。
- Access level (访问级别) - 为存储桶授予的访问权限：
  - List (列出) - 列出资源。
  - Read (读取) - 读取但不编辑资源内容和属性。
  - Write (写入) - 创建、删除或修改资源。
  - Permissions (权限) - 授予或修改资源权限。
  - Tagging (标记) - 更新与资源关联的标记。

启用 S3 访问分析器

要使用 S3 访问分析器，您必须完成以下必备步骤。

1. 授予所需的权限。

   有关更多信息，请参阅《IAM 用户指南》中的使用访问分析器所需的权限。
2. 请访问 IAM 以便为要使用访问分析器的每个区域创建账户级分析器。

   S3 访问分析器需要账户级分析器。要使用 S3 访问分析器，您必须创建具有一个账户作为信任区域的分析器。有关更多信息，请参阅《IAM 用户指南》中的启用访问分析器。

阻止所有公有访问

如果您想要通过单击一次来阻止对存储桶的所有访问，则可以使用 S3 访问分析器中的 Block all public access (阻止所有公有访问) 按钮。当您阻止对存储桶的所有公有访问时，系统不会授予公有访问权限。我们建议您阻止所有对存储桶的公有访问，除非您需要公有访问才能支持特定和经验证的使用案例。在阻止所有公有访问之前，请确保您的应用程序在没有公有访问权限的情况下可以继续正常工作。

如果您不想阻止对存储桶的所有公有访问，则可以在 Amazon S3 控制台上编辑阻止公有访问设置，以配置存储桶的精细访问级别。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 阻止公有访问。

在极少数情况下，对于 Amazon S3 阻止公有访问评估报告为公有的存储桶，S3 访问分析器可能不会报告任何结果。发生这种情况的原因是，Amazon S3 阻止公有访问会审核当前操作以及将来可能添加的任何潜在操作的策略，从而导致存储桶变为公有。另一方面，S3 访问分析器只分析在评估访问状态时为 Amazon S3 服务指定的当前操作。

使用 S3 访问分析器阻止对存储桶的所有公有访问

1. 登录 AWS 管理控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中的 Dashboards (控制面板) 下，选择 Access analyzer for S3 (S3 访问分析器)。
3. 在 S3 访问分析器中，选择一个存储桶。
4. 选择 Block all public access (阻止所有公有访问)。
5. 要确认您阻止对存储桶的所有公有访问的意图，请在 Block all public access (bucket settings) [阻止所有公有访问（存储桶设置）] 中输入 **`confirm`**。

   Amazon S3 会阻止对存储桶的所有公有访问。存储桶结果的状态更新为 resolved (已解决)，并且存储桶从 S3 访问分析器列表中消失。如果要查看已解决的存储桶，请在 IAM 控制台上打开 IAM 访问分析器。

查看和更改存储桶访问权限

如果您不打算对公有账户或其他 AWS 账户（包括组织外部的账户）授予访问权限，则可以修改存储桶 ACL、存储桶策略或访问点策略来删除对存储桶的访问权限。Shared through (共享方式) 列显示存储桶访问权限的所有来源：存储桶策略、存储桶 ACL 和/或访问点策略。

查看和更改存储桶策略、存储桶 ACL 或访问点策略

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择 Access analyzer for S3 (S3 访问分析器)。
3. 要查看是否已通过存储桶策略、存储桶 ACL 或访问点策略授予公有访问权限或共享访问权限，请查看 Shared through (共享方式) 列。
4. 在 Buckets (存储桶) 下，选择您想要更改或查看其存储桶策略、存储桶 ACL 或访问点策略的存储桶的名称。
5. 如果要更改或查看存储桶 ACL：

   a. 选择 Permissions。

   b. 选择访问控制列表。

   c. 查看您的存储桶 ACL，并根据需要进行更改。

   有关更多信息，请参阅 如何设置 ACL 存储桶权限？ (p. 58)。
6. 如果要更改或查看存储桶策略：

   a. 选择 Permissions。

   b. 选择存储桶策略。

   c. 根据需要查看或更改存储桶策略。

   有关更多信息，请参阅 如何添加 S3 存储桶策略？ (p. 59)。
7. 如果要查看或更改访问点策略：

   a. 选择 Access points (访问点)。

   b. 选择访问点名称。

   c. 根据需要查看或更改访问权限。

   有关更多信息，请参阅 管理和使用 Amazon S3 访问点 (p. 20)。

   如果您编辑或删除存储桶 ACL、存储桶策略或访问点策略以删除公有访问或共享访问权限，则存储桶结果的状态会更新为已解决。已解决的存储桶结果从 S3 访问分析器列表中消失，但您可以在 IAM 访问分析器中查看它们。

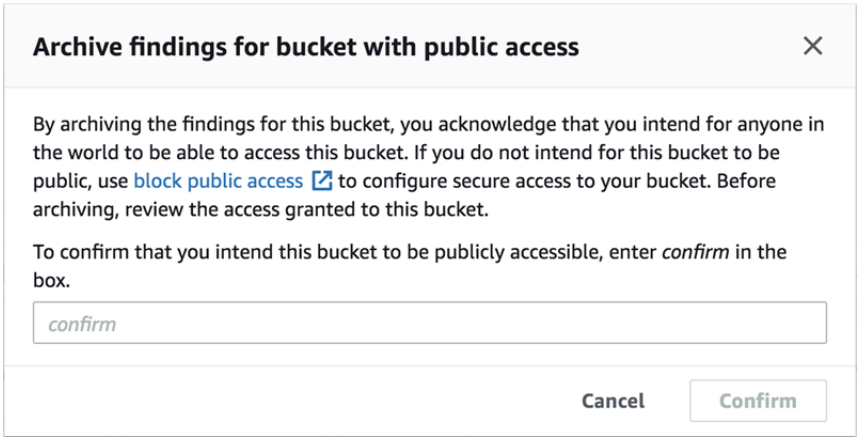
对存储桶结果进行存档

如果存储桶对公共账户或其他 AWS 账户（包括组织外部的账户）授予访问权限，以便支持特定使用案例（例如，静态网站、公共下载或跨账户共享），则可以存档该存储桶的结果。当您对存储桶结果进行存档时，即表示您确认并记录存储桶保持公开或共享的意图。已存档的存储桶结果将保留在您的 S3 访问分析器列表中，以便您始终知道哪些存储桶是公有存储桶或共享存储桶。

在 S3 访问分析器中存档存储桶结果

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择 Access analyzer for S3 (S3 访问分析器)。

3. 在 S3 访问分析器中，选择一个活动存储桶。
4. 要确认您想让公共账户或其他 AWS 账户（包括组织外部的账户）访问此存储桶的意图，请选择 Archive (存档)。
5. 输入 **`confirm`**，然后选择 Archive (存档)。



激活已存档的存储桶结果

对结果进行存档后，您可以随时重新访问这些结果并将其状态更改回活动状态，这表明存储桶需要另一次审核。

在 S3 访问分析器中激活存档存储桶结果

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择 Access analyzer for S3 (S3 访问分析器)。
3. 选择已存档的存储桶结果。
4. 选择 Mark as active (标记为活动)。

查看结果详细信息

如果您需要查看有关存储桶的更多信息，可以在 IAM 控制台的 IAM 访问分析器中打开存储桶结果详细信息。

在 S3 访问分析器中查看结果详细信息

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择 Access analyzer for S3 (S3 访问分析器)。
3. 在 S3 访问分析器中，选择一个存储桶。
4. 选择查看详细信息。

   结果详细信息将在 IAM 控制台的 IAM 访问分析器中打开。

下载 S3 访问分析器报告

您可以将存储桶结果下载为 CSV 格式的报告，供审计使用。该报告包含的信息与您在 Amazon S3 控制台的 S3 访问分析器中看到的信息相同。

下载报告

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧的导航窗格中，选择 Access analyzer for S3 (S3 访问分析器)。
3. 在“Region (区域)”筛选器中，选择相应的区域。

   S3 访问分析器会更新以显示所选区域的存储桶。
4. 选择 Download report (下载报告)。

   系统会生成 CSV 报告并保存到您的计算机中。

文档历史记录

文档最新更新时间：2019 年 3 月 27 日

下表描述了自 2018 年 6 月 19 日之后的每个《Amazon Simple Storage Service 控制台用户指南》版本中的重要更改。如需对此文档更新的通知，您可以订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
新存档存储类 (p. 67)	Amazon S3 现在提供了用于存储很少访问的对象的新存档存储类 S3 Glacier Deep Archive。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的如何还原已存档的 S3 对象？和存储类。	2019 年 3 月 27 日
阻止对 S3 存储桶的公有访问 (p. 67)	Amazon S3 阻止公有访问将阻止使用允许对 S3 存储桶中的数据进行公有访问的任何设置的应用程序。有关更多信息，请参阅阻止对 S3 存储桶的公有访问。	2018 年 11 月 15 日
跨区域复制 (CRR) 规则中的筛选增强功能 (p. 67)	在 CRR 规则中，您可以指定对象筛选器以选择要将向其应用规则的对象子级。以前，您只能按对象键前缀进行筛选。在本版本中，您可以按对象键前缀和/或一个或多个对象标签进行筛选。有关更多信息，请参阅如何向 S3 存储桶添加复制规则？	2018 年 9 月 19 日
现在可通过 RSS 更新 (p. 67)	现在您可以订阅 RSS 源来接收有关《Amazon Simple Storage Service 控制台用户指南》更新的通知。	2018 年 19 月 6 日

早期更新

下表描述了自 2018 年 6 月 19 日之前的每个《Amazon Simple Storage Service 控制台用户指南》版本中的重要更改。

变更	描述	更改日期
新存储类别	Amazon S3 现在提供了用于存储对象的新存储类 ONEZONE_IA（IA，适用于不频繁访问）。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的存储类。	2018 年 4 月 4 日
支持 ORC 格式 Amazon S3 清单文件	对于清单输出文件，除了逗号分隔值 (CSV) 文件格式之外，Amazon S3 现在还支持 Apache 优化行列式 (ORC) 格式。有关更多信息，请参阅如何配置 Amazon S3 清单？ (p. 48)。	2017 年 11 月 17 日

变更	描述	更改日期
存储桶权限检查	Amazon S3 控制台中的存储桶权限检查会检查存储桶策略和存储桶访问控制列表 (ACL)，从而识别可公开访问的存储桶。存储桶权限检查使得识别提供公开读取和写入访问权的 S3 存储桶更加简单。 .	2017 年 11 月 06 日
S3 存储桶的默认加密	Amazon S3 默认加密提供了一种方法来设置 S3 存储桶的默认加密行为。您可以对存储桶设置默认加密，以便在存储桶中存储所有对象时对这些对象进行加密。这些对象使用 Amazon S3 托管密钥 (SSE-S3) 或 AWS KMS 托管密钥 (SSE-KMS) 通过服务器端加密进行加密。有关更多信息，请参阅 如何为 Amazon S3 存储桶启用默认加密？ (p. 7)。	2017 年 11 月 06 日
Amazon S3 清单中的加密状态	Amazon S3 现在的支持包括 Amazon S3 清单中的加密状态，因此您查看对象在静态时如何加密，以用于合规性审计或其他用途。您还可以配置使用服务器端加密 (SSE) 或 SSE-KMS 来加密 Amazon S3 清单，从而相应地加密所有清单文件。有关更多信息，请参阅 如何配置 Amazon S3 清单？ (p. 48)。	2017 年 11 月 06 日
跨区域复制增强功能	跨区域复制现在支持以下功能： • 默认情况下，Amazon S3 不复制您的源存储桶中使用 AWS KMS 托管密钥通过服务器端加密创建的对象。现在您可以配置复制规则来复制这些对象。有关更多信息，请参阅 如何向 S3 存储桶添加复制规则？ (p. 43)。 • 在跨账户方案中，您可以配置复制规则，将副本所有权更改为拥有目标存储桶的 AWS 账户。有关更多信息，请参阅 如何向 S3 存储桶添加复制规则？ (p. 43)。	2017 年 11 月 06 日
增加了功能和文档	Amazon S3 控制台现在支持使用 AWS CloudTrail 数据事件日志记录为 S3 存储桶启用对象级别日志记录。有关更多信息，请参阅 如何使用 AWS CloudTrail 数据事件为 S3 存储桶启用对象级别日志记录？ (p. 9)。	2017 年 10 月 19 日
旧版 Amazon S3 控制台不再可用	旧版 Amazon S3 控制台不再可用，已从 Amazon S3 文档站点中删除旧版用户指南。	2017 年 8 月 31 日
新的 Amazon S3 控制台正式发布	宣布正式发布新的 Amazon S3 控制台。	2017 年 5 月 15 日

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 一般参考》中的 AWS 词汇表。