



## 管理 **S3** 访问密钥

### StorageGRID software

NetApp  
July 23, 2026

# 目录

- 管理 S3 访问密钥 ..... 1
  - 管理 StorageGRID 中的 S3 访问密钥 ..... 1
  - 在 StorageGRID 中创建您自己的 S3 访问密钥 ..... 1
  - 在 StorageGRID 中查看您的 S3 访问密钥 ..... 2
  - 在 StorageGRID 中删除您自己的 S3 访问密钥 ..... 3
  - 在 StorageGRID 中创建其他用户的 S3 访问密钥 ..... 3
  - 在 StorageGRID 中查看其他用户的 S3 访问密钥 ..... 4
  - 在 StorageGRID 中删除其他用户的 S3 访问密钥 ..... 5

# 管理 S3 访问密钥

## 管理 StorageGRID 中的 S3 访问密钥

S3 租户帐户的每个用户都必须有一个访问密钥，才能在 StorageGRID 系统中存储和检索对象。访问密钥由访问密钥 ID 和秘密访问密钥组成。

S3 访问密钥可以按以下方式管理：

- 拥有\*管理您自己的 S3 凭据\*权限的用户可以创建或删除自己的 S3 访问密钥。
- 拥有 **Root access** 权限的用户可以管理 S3 根帐户和所有其他用户的访问密钥。根访问密钥为租户提供对所有存储桶和对象的完全访问权限，除非存储桶策略明确禁用。

StorageGRID 支持签名版本 2 和签名版本 4 身份验证。除非存储桶策略明确启用，否则不允许跨帐户访问。

## 在 StorageGRID 中创建您自己的 S3 访问密钥

如果使用的是 S3 租户，并且拥有相应的权限，则可以创建自己的 S3 访问密钥。您必须拥有访问密钥才能访问存储桶和对象。

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到租户管理器。
- 您属于具有 ["管理自己的 S3 凭据或根访问权限"](#) 的用户组。

关于此任务

您可以创建一个或多个 S3 访问密钥，允许您为租户帐户创建和管理存储桶。创建新的访问密钥后，使用新的访问密钥 ID 和机密访问密钥更新应用程序。出于安全考虑，请勿创建超出所需数量的密钥，并删除未使用的密钥。如果您只有一个密钥并且即将过期，请在旧密钥过期之前创建一个新密钥，然后删除旧密钥。

每个密钥可以有特定的到期时间或没有到期时间。请遵循以下有关到期时间的准则：

- 设置密钥的到期时间，将访问权限限制为特定时间段。设置较短的到期时间有助于降低您的访问密钥 ID 和秘密访问密钥意外泄露的风险。过期的密钥将自动删除。
- 如果环境中的安全风险较低，并且不需要定期创建新密钥，则无需为密钥设置过期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。



可以使用租户管理器中为您的帐户显示的访问密钥 ID 和密钥访问属于您的帐户的 S3 存储桶和对象。为此，请像保护密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并切勿与其他用户共享这些密钥。

步骤

1. 选择 **STORAGE (S3) > My access keys**。

此时将显示我的访问密钥页面，并列出任何现有的访问密钥。

2. 选择\*创建密钥\*。

3. 执行以下操作之一：

- 选择\*不设置过期时间\*以创建不会过期的密钥。（默认）
- 选择\*设置到期时间\*，然后设置到期日期和时间。



到期日期最长可为自当前日期起五年。到期时间最短可为自当前时间起一分钟。

4. 选择\*创建访问密钥\*。

此时将显示下载访问密钥对话框，其中列出了您的访问密钥 ID 和秘密访问密钥。

5. `${post_edited_translations.segment}`



在复制或下载此信息之前，请勿关闭此对话框。对话框关闭后，您将无法复制或下载密钥。

6. 选择 **Finish**。

新密钥列在“我的访问密钥”页面上。

7. 如果您的租户帐户具有\*使用网格联合连接\*权限，则可以选择使用租户管理 API 手动将 S3 访问密钥从源网格上的租户克隆到目标网格上的租户。请参阅 [“使用 API 克隆 S3 访问密钥”](#)。

## 在 StorageGRID 中查看您的 S3 访问密钥

如果使用的是 S3 租户并且具有[“适当的权限”](#)，则可以查看 S3 访问密钥的列表。您可以按到期时间对列表进行排序，以便确定哪些密钥即将到期。根据需要，您可以[“创建新密钥”](#)或[“删除密钥”](#)不再使用的密钥。



可以使用租户管理器中为您的帐户显示的访问密钥 ID 和密钥访问属于您的帐户的 S3 存储桶和对象。为此，请像保护密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并切勿与其他用户共享这些密钥。

### 开始之前

- 您已使用 [“支持的 Web 浏览器”](#) 登录到租户管理器。
- 您属于具有“管理您自己的 S3 凭据”的用户组 [“权限”](#)。

### 步骤

1. 选择 **STORAGE (S3) > My access keys**。
2. 在“我的访问密钥”页面中，按\*到期时间\*或\*访问密钥 ID\*对任何现有访问密钥进行排序。
3. 根据需要，创建新密钥或删除不再使用的密钥。

如果在现有密钥过期之前创建新密钥，则可以开始使用新密钥，而不会暂时失去对帐户中对象的访问权限。

过期的密钥将自动删除。

## 在 StorageGRID 中删除您自己的 S3 访问密钥

如果使用的是 S3 租户，并且拥有相应的权限，则可以删除自己的 S3 访问密钥。删除访问密钥后，它不能再用于访问租户帐户中的对象和存储桶。

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到租户管理器。
- 您有 ["管理自己的 S3 凭据权限"](#)。



可以使用租户管理器中为您的帐户显示的访问密钥 ID 和密钥访问属于您的帐户的 S3 存储桶和对象。为此，请像保护密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并切勿与其他用户共享这些密钥。

步骤

1. 选择 **STORAGE (S3) > My access keys**。
2. 在"我的访问密钥"页面中，选中要删除的每个访问密钥的复选框。
3. 选择\*Delete key\*。
4. 在确认对话框中，选择\*Delete key\*。

页面右上角会显示一条确认消息。

## 在 StorageGRID 中创建其他用户的 S3 访问密钥

如果使用的是 S3 租户并且具有适当的权限，则可以为其他用户创建 S3 访问密钥，例如需要访问存储区和对象的应用程序。

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到租户管理器。
- 您属于具有 ["root 访问权限"](#) 的用户组。

关于此任务

您可以为其他用户创建一个或多个 S3 访问密钥，以便他们可以为其他租户帐户创建和管理存储桶。创建新的访问密钥后，使用新的访问密钥 ID 和机密访问密钥更新应用程序。出于安全考虑，请勿创建超出用户需要的密钥，并删除未使用的密钥。如果您只有一个密钥，并且即将过期，请在旧密钥过期之前创建一个新密钥，然后删除旧密钥。

每个密钥可以有特定的到期时间或没有到期时间。请遵循以下有关到期时间的准则：

- 设置密钥的到期时间，以将用户的访问权限限制为特定时间段。设置较短的到期时间有助于降低访问密钥 ID 和秘密访问密钥意外泄露的风险。过期的密钥将自动删除。
- 如果环境中的安全风险较低，并且不需要定期创建新密钥，则无需为密钥设置过期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。



可以使用租户管理器中为该用户显示的访问密钥 ID 和机密访问密钥来访问属于该用户的 S3 存储桶和对象。为此，请像保护密码一样保护访问密钥。定期轮换访问密钥，从账户中删除所有未使用的密钥，切勿与其他用户共享密钥。

#### 步骤

1. 选择\*访问管理\* > 用户。
2. 选择要管理其 S3 访问密钥的用户。

此时将显示用户详细信息页面。

3. 选择 **Access keys**，然后选择 **Create key**。
4. 执行以下操作之一：
  - 选择\*不要设置过期时间\*以创建不会过期的密钥。（默认）
  - 选择\*设置到期时间\*，然后设置到期日期和时间。



到期日期最长可为自当前日期起五年。到期时间最短可为自当前时间起一分钟。

5. 选择\*创建访问密钥\*。

此时将显示"下载访问密钥"对话框，其中列出了访问密钥 ID 和秘密访问密钥。

6. `${post_edited_translations.segment}`



在复制或下载此信息之前，请勿关闭此对话框。对话框关闭后，您将无法复制或下载密钥。

7. 选择 **Finish**。

新密钥列在用户详细信息页面的访问密钥选项卡上。

8. 如果您的租户帐户具有\*使用网格联合连接\*权限，则可以选择使用租户管理 API 手动将 S3 访问密钥从源网格上的租户克隆到目标网格上的租户。请参阅 ["使用 API 克隆 S3 访问密钥"](#)。

## 在 StorageGRID 中查看其他用户的 S3 访问密钥

如果使用的是 S3 租户并且具有适当的权限，则可以查看其他用户的 S3 访问密钥。您可以按到期时间对列表进行排序，以便确定哪些密钥即将到期。根据需要，您可以创建新密钥并删除不再使用的密钥。

#### 开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到租户管理器。
- 您有 ["root 访问权限"](#)。



可以使用租户管理器中为该用户显示的访问密钥 ID 和机密访问密钥来访问属于该用户的 S3 存储桶和对象。为此，请像保护密码一样保护访问密钥。定期轮换访问密钥，从账户中删除所有未使用的密钥，切勿与其他用户共享密钥。

## 步骤

1. 选择\*访问管理\* > 用户。
2. 从"用户"页面中，选择要查看其 S3 访问密钥的用户。
3. 在用户详细信息页面中，选择\*访问密钥\*。
4. 按\*到期时间\*或\*访问密钥 ID\*对密钥进行排序。
5. 根据需要，创建新密钥并手动删除不再使用的密钥。

如果在现有密钥过期之前创建新密钥，用户可以开始使用新密钥，而不会暂时失去对帐户中对象的访问权限。

过期的密钥将自动删除。

## 相关信息

- ["创建其他用户的 S3 访问密钥"](#)
- ["删除其他用户的 S3 访问密钥"](#)

# 在 StorageGRID 中删除其他用户的 S3 访问密钥

如果使用的是 S3 租户并且具有适当的权限，则可以删除其他用户的 S3 访问密钥。删除访问密钥后，它不能再用于访问租户帐户中的对象和存储桶。

## 开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到租户管理器。
- 您有 ["root 访问权限"](#)。



可以使用租户管理器中为该用户显示的访问密钥 ID 和机密访问密钥来访问属于该用户的 S3 存储桶和对象。为此，请像保护密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除所有未使用的密钥，切勿与其他用户共享密钥。

## 步骤

1. 选择\*访问管理\* > 用户。
2. 从"用户"页面中，选择要管理其 S3 访问密钥的用户。
3. 在"用户详细信息"页面中，选择 **Access keys**，然后选中要删除的每个访问密钥的复选框。
4. 选择\*操作\* > 删除所选键。
5. 在确认对话框中，选择\*Delete key\*。

页面右上角会显示一条确认消息。

## 版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。