



使用网格联合连接 StorageGRID 11.8

NetApp
March 19, 2024

目录

使用网格联合连接	1
克隆租户组 and 用户	1
使用API克隆S3访问密钥	5
管理跨网格复制	7
查看网格联合连接	12

使用网格联合连接

克隆租户组 and 用户

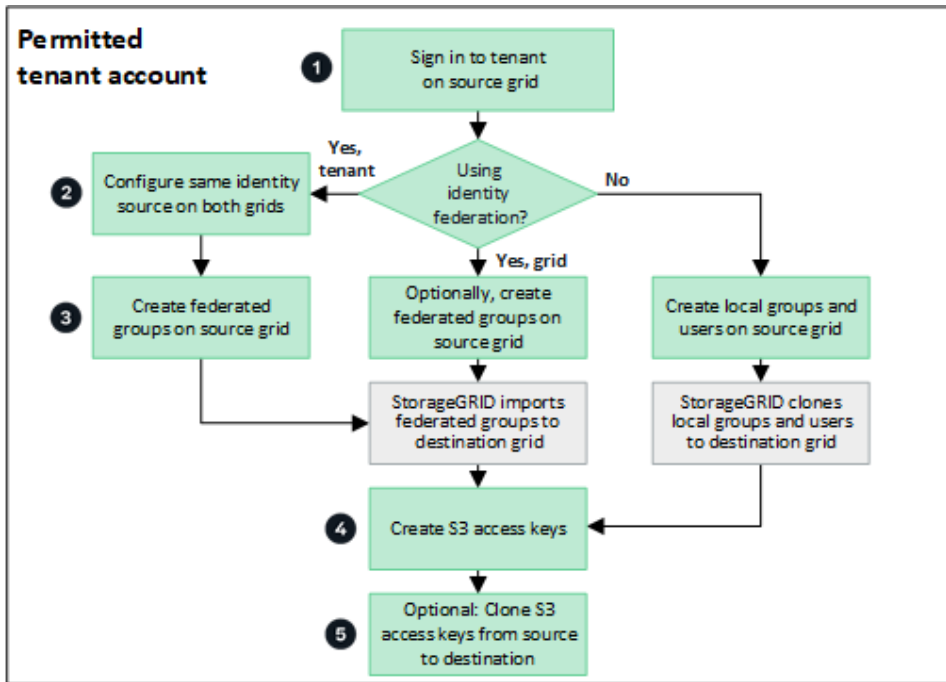
如果创建或编辑租户以使用网格联合连接、则会将该租户从一个StorageGRID系统(源租户)复制到另一个StorageGRID系统(副本租户)。复制租户后、添加到源租户的任何组和用户都会克隆到副本租户。

最初创建租户的StorageGRID系统是租户的 `_source grid_`。复制租户的StorageGRID系统是租户的 `_Destination grid_`。这两个租户帐户具有相同的帐户ID、名称、问题描述、存储配额和已分配权限、但是、目标租户最初没有root用户密码。有关详细信息，请参见 ["什么是帐户克隆"](#) 和 ["管理允许的租户"](#)。

需要克隆租户帐户信息 ["跨网格复制"](#) 存储分段对象数。在两个网格上使用相同的租户组和用户可确保您可以访问任一网格上的相应分段和对象。

帐户克隆的租户工作流

如果您的租户帐户具有*使用网格联合连接*权限、请查看工作流示意图、了解克隆组、用户和S3访问密钥要执行的步骤。



以下是工作流中的主要步骤：

1 登录到租户

登录到源网格(最初创建租户的网格)上的租户帐户。

2 (可选)配置身份联合

如果您的租户帐户具有*使用自己的身份源*权限来使用联盟组 and 用户、请为源租户帐户和目标租户帐户配置相同的身份源(设置相同)。除非两个网格使用同一身份源、否则无法克隆联盟组和用户。有关说明,请参见 ["使用身份联合"](#)。

3

创建组 and 用户

创建组 and 用户时、请始终从租户的源网格开始。添加新组时、StorageGRID 会自动将其克隆到目标网格。

- 如果为整个StorageGRID 系统 or 租户帐户配置了身份联合、["创建新租户组"](#) 从身份源导入联盟组。
- 如果您不使用联合身份验证、["创建新的本地组"](#) 然后 ["创建本地用户"](#)。

4

创建S3访问密钥

您可以 ["创建您自己的访问密钥"](#) 或至 ["创建其他用户的访问密钥"](#) 在源网格 or 目标网格上访问该网格上的存储分段。

5

(可选)克隆S3访问密钥

如果您需要访问两个网格上具有相同访问密钥的分段、请在源网格上创建访问密钥、然后使用租户管理器API手动将其克隆到目标网格。有关说明,请参见 ["使用API克隆S3访问密钥"](#)。

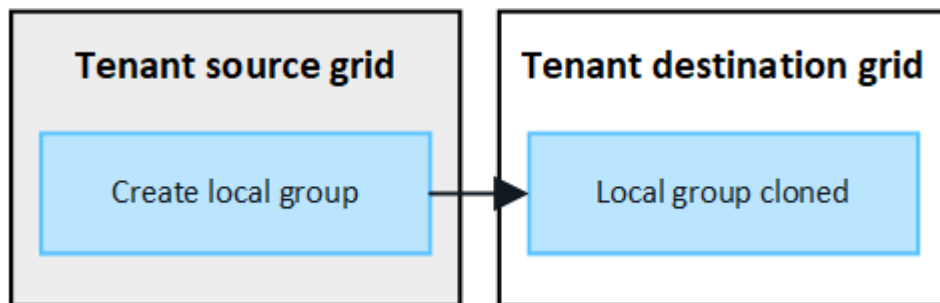
如何克隆组、用户 and S3访问密钥?

查看本节、了解如何在租户源网格 and 租户目标网格之间克隆组、用户 and S3访问密钥。

克隆在源网格上创建的本地组

创建租户帐户并将其复制到目标网格后、StorageGRID 会自动将您添加到租户源网格的任何本地组克隆到租户的目标网格。

原始组及其克隆具有相同的访问模式、组权限 and S3组策略。有关说明,请参见 ["为 S3 租户创建组"](#)。

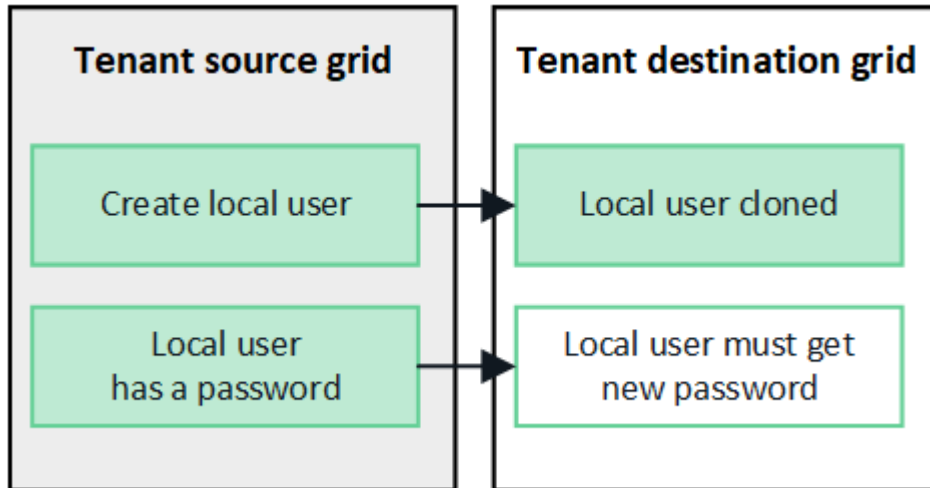


在源网格上创建本地组时选择的任何用户、在将组克隆到目标网格时均不包括在内。因此、请勿在创建组时选择用户。而是在创建用户时选择组。

克隆在源网格上创建的本地用户

在源网格上创建新的本地用户时、StorageGRID 会自动将该用户克隆到目标网格。原始用户及其克隆具有相同的全名、用户名 and *deny access* 设置。这两个用户也属于相同的组。有关说明,请参见 ["管理本地用户"](#)。

出于安全原因、本地用户密码不会克隆到目标网格。如果本地用户需要访问目标网格上的租户管理器、租户帐户的root用户必须在目标网格上为该用户添加密码。有关说明，请参见 ["管理本地用户"](#)。

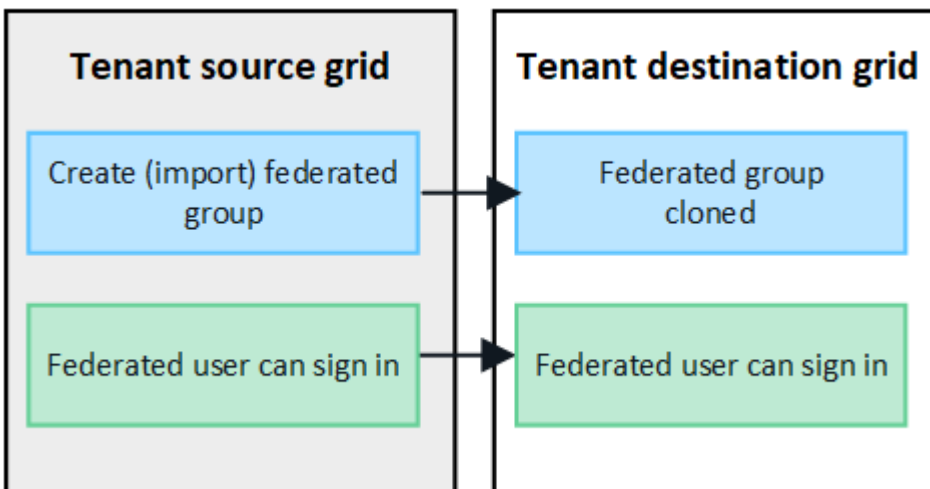


克隆在源网格上创建的联盟组

假设需要将帐户克隆与结合使用 ["单点登录"](#) 和 ["身份联合"](#) 满足此条件后、您在源网格上为租户创建(导入)的联合组将自动克隆到目标网格上的租户。

这两个组具有相同的访问模式、组权限和S3组策略。

为源租户创建联盟组并克隆到目标租户后、联盟用户可以在任一网格上登录到租户。

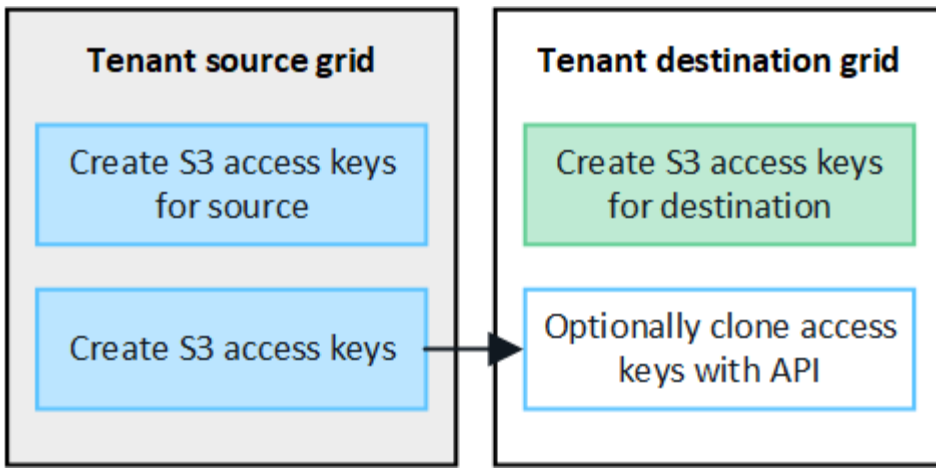


可以手动克隆S3访问密钥

StorageGRID 不会自动克隆S3访问密钥、因为通过在每个网格上使用不同的密钥可以提高安全性。

要管理两个网格上的访问密钥、您可以执行以下任一操作：

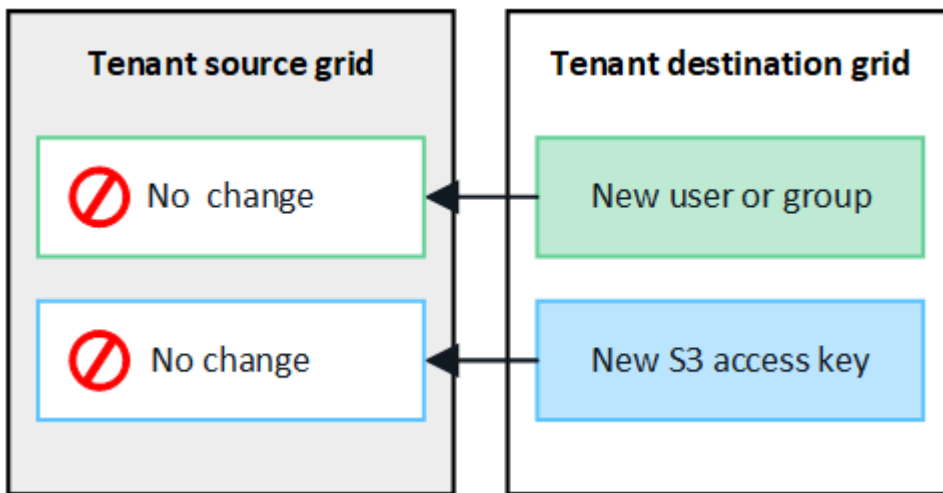
- 如果您不需要对每个网格使用相同的键、则可以使用 ["创建您自己的访问密钥"](#) 或 ["创建其他用户的访问密钥"](#) 在每个网格上。
- 如果需要在两个网格上使用相同的密钥、可以在源网格上创建密钥、然后使用租户管理器API手动创建 ["克隆密钥"](#) 到目标网格。



克隆联盟用户的S3访问密钥时、用户和S3访问密钥都会克隆到目标租户。

添加到目标网格的组和用户不会进行克隆

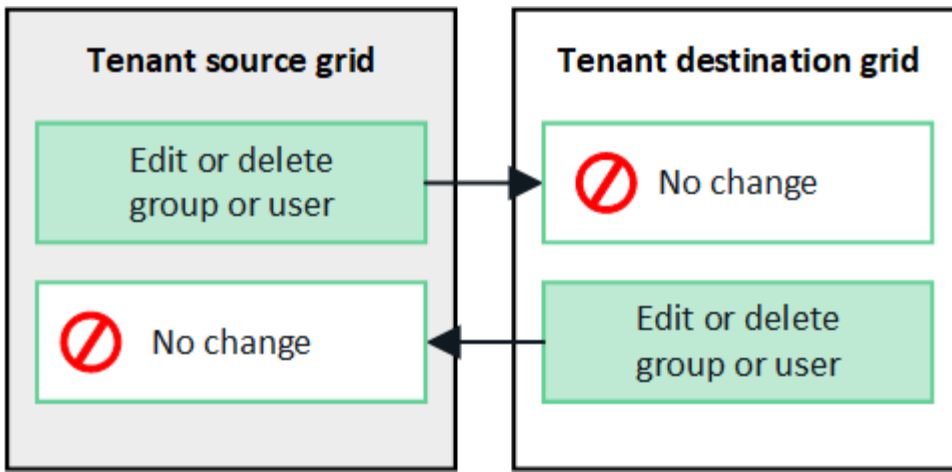
只会从租户的源网格克隆到租户的目标网格。如果在租户的目标网格上创建或导入组和用户、StorageGRID 不会将这些项克隆回租户的源网格。



编辑或删除的组、用户和访问密钥不会克隆

只有在创建新组 and 用户时、才会进行克隆。

如果编辑或删除任一网格上的组、用户或访问密钥、则所做的更改不会克隆到另一个网格。



使用API克隆S3访问密钥

如果您的租户帐户具有*使用网格联合连接*权限、则可以使用租户管理API将S3访问密钥从源网格上的租户手动克隆到目标网格上的租户。

开始之前

- 租户帐户具有*使用网格联合连接*权限。
- 网格联合连接的*连接状态*为*已连接*。
- 您已使用登录到租户源网格上的租户管理器 [支持的 Web 浏览器](#)。
- 您属于具有的用户组 [管理您自己的S3凭据或root访问权限](#)。
- 如果要克隆本地用户的访问密钥、则该用户已位于两个网格上。



克隆联盟用户的S3访问密钥时、用户和S3访问密钥都会添加到目标租户。

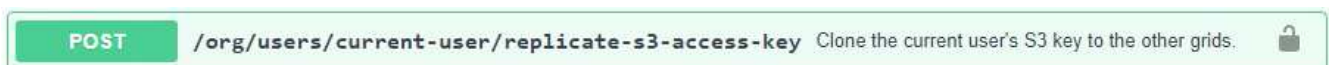
克隆您自己的访问密钥

如果需要访问两个网格上的相同分段、可以克隆自己的访问密钥。

步骤

1. 在源网格上使用租户管理器、["创建您自己的访问密钥"](#) 并下载 .csv 文件
2. 从租户管理器的顶部、选择帮助图标并选择* API文档*。
3. 在*S3*部分中、选择以下端点：

```
POST /org/users/current-user/replicate-s3-access-key
```



4. 选择 * 试用 *。
5. 在*body文本框中、将*accessKey*和*sretAccessKey*的示例条目替换为您下载的*.csv文件中的值。

请务必在每个字符串周围保留双引号。



6. 如果密钥将过期，请将*expires*的示例条目替换为ISO 8601数据时间格式的字符串(例如， 2024-02-28T22:46:33-08:00)。如果密钥不会过期，请输入*null*作为*expires*条目的值(或删除*expires*行和前面的逗号)。
7. 选择 * 执行 *。
8. 确认服务器响应代码为*204*，表示密钥已成功克隆到目标网格。

克隆其他用户的访问密钥

如果其他用户需要访问两个网格上的相同分段、则可以克隆其访问密钥。

步骤

1. 在源网格上使用租户管理器、"[创建其他用户的S3访问密钥](#)"并下载 .csv 文件
2. 从租户管理器的顶部、选择帮助图标并选择* API文档*。
3. 获取用户ID。您需要此值来克隆其他用户的访问密钥。
 - a. 从*USERS*部分中，选择以下端点：

```
GET /org/users
```
 - b. 选择 * 试用 *。
 - c. 指定查找用户时要使用的任何参数。
 - d. 选择 * 执行 *。
 - e. 找到要克隆其密钥的用户，然后在*id*字段中复制该数字。
4. 在*S3*部分中，选择以下端点：

```
POST /org/users/{userId}/replicate-s3-access-key
```



5. 选择 * 试用 *。
6. 在*userId*文本框中，粘贴您复制的用户ID。
7. 在*body*文本框中，将*示例访问密钥*和*机密访问密钥*的示例条目替换为该用户的*.csv*文件中的值。

请务必在字符串周围保留双引号。

8. 如果密钥将过期，请将*expires*的示例条目替换为ISO 8601数据时间格式的字符串(例如， 2023-02-

28T22:46:33-08:00) 。如果密钥不会过期，请输入*null*作为*expires*条目的值(或删除*expires*行和前面的逗号)。

9. 选择 * 执行 * 。

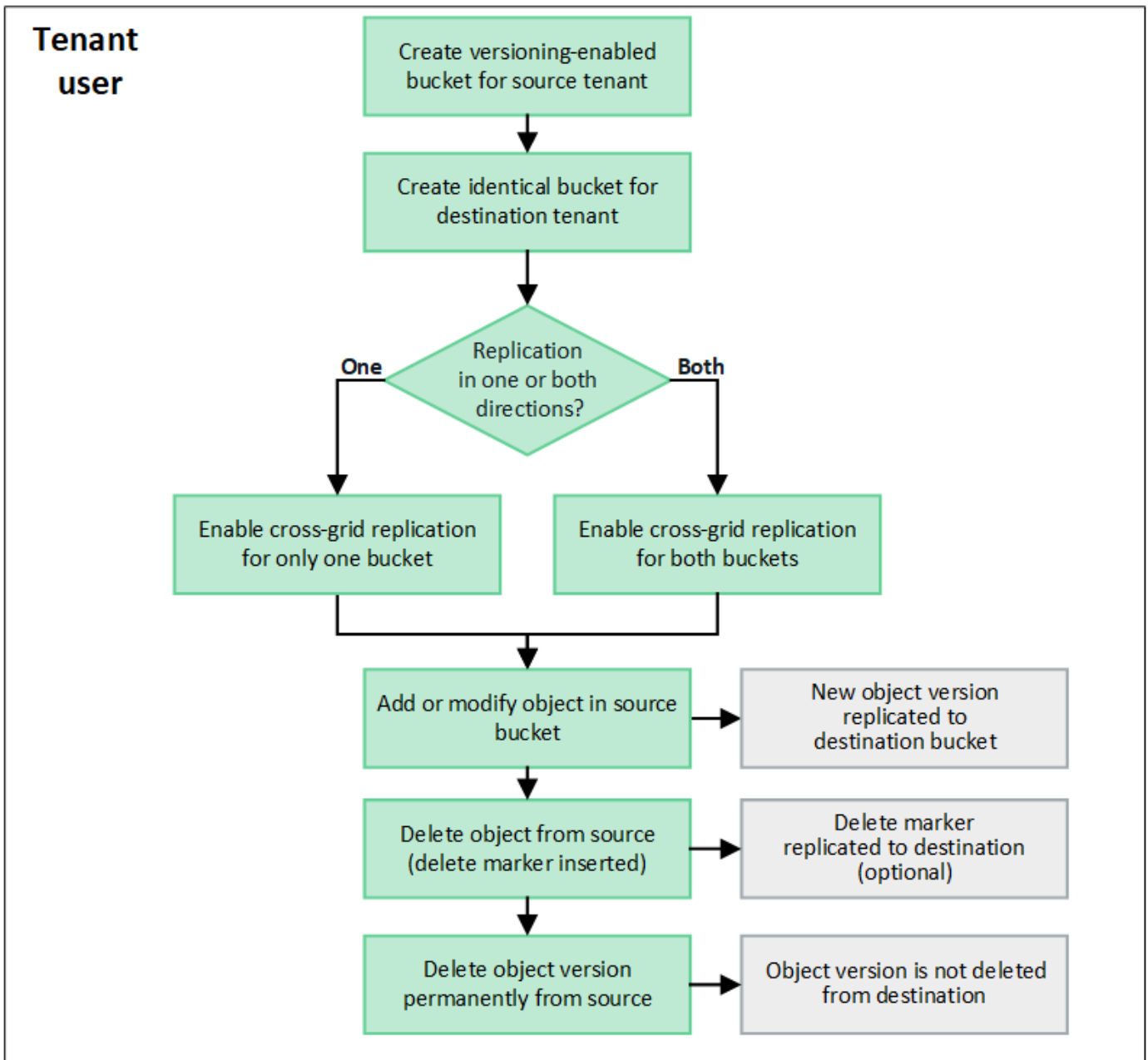
10. 确认服务器响应代码为*204*，表示密钥已成功克隆到目标网格。

管理跨网格复制

如果在创建租户帐户时为其分配了*使用网格联合连接*权限、则可以使用跨网格复制在租户源网格上的分段和租户目标网格上的分段之间自动复制对象。跨网格复制可以在一个方向或两个方向上进行。

跨网格复制 workflow

此 workflow 图汇总了在两个网格上的分段之间配置跨网格复制所要执行的步骤。下面将详细介绍这些步骤。



配置跨网格复制

在使用跨网格复制之前、您必须登录到每个网格上的相应租户帐户并创建相同的分段。然后、您可以在一个存储分段或这两个存储分段上启用跨网格复制。

开始之前

- 您已查看跨网格复制的要求。请参见 ["什么是跨网格复制"](#)。
- 您正在使用 ["支持的 Web 浏览器"](#)。
- 租户帐户具有*使用网格联合连接*权限、两个网格上都存在相同的租户帐户。请参见 ["管理网格联盟连接允许的租户"](#)。
- 您要登录的租户用户已位于两个网格上、并且属于具有的用户组 ["root访问权限"](#)。
- 如果您要以本地用户身份登录到租户的目标网格、则租户帐户的root用户已为此网格上的用户帐户设置密码。

创建两个相同的存储分段

首先、登录到每个网格上的相应租户帐户并创建相同的分段。

步骤

1. 从网格联合连接中的任一网格开始、创建一个新存储分段：

a. 使用两个网格上的租户用户凭据登录到租户帐户。



如果您无法以本地用户身份登录到租户的目标网格、请确认租户帐户的root用户已为您的用户帐户设置密码。

b. 按照说明进行操作 "[创建S3存储分段](#)"。

c. 在*管理对象设置*选项卡上，选择*启用对象版本控制*。

d. 如果为StorageGRID 系统启用了S3对象锁定、请勿为此存储分段启用S3对象锁定。

e. 选择 * 创建存储分段 *。

f. 选择 * 完成 *。

2. 重复这些步骤、为网格联盟连接中另一个网格上的同一租户帐户创建相同的分段。



根据需要、每个存储分段可以使用不同的区域。

启用跨网格复制

在向任一存储分段添加任何对象之前、必须执行这些步骤。

步骤

1. 从要复制其对象的网格开始、启用 "[跨网格单向复制](#)"：

a. 登录到存储分段的租户帐户。

b. 从信息板中选择*查看存储分段*，或选择*存储(S3)*>*存储分段*。

c. 从表中选择存储分段名称以访问存储分段详细信息页面。

d. 选择*跨网格复制*选项卡。

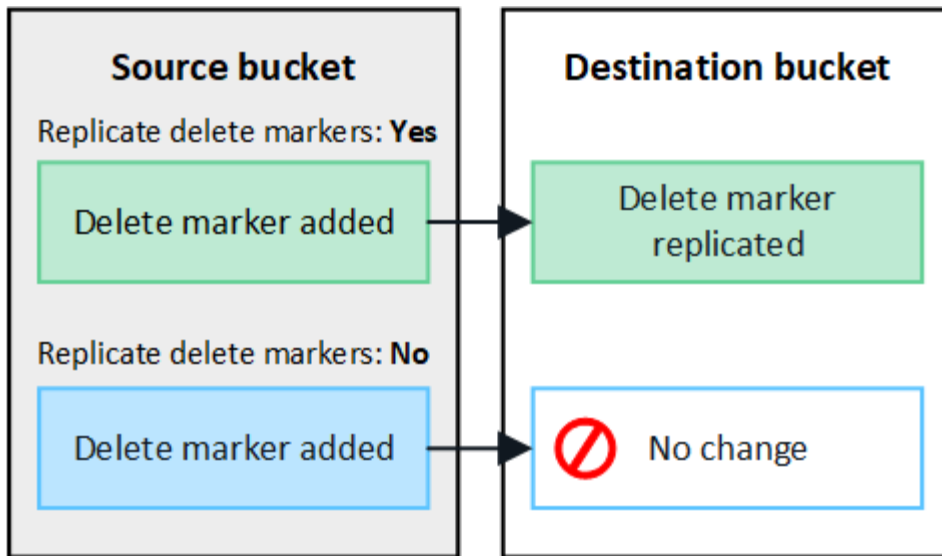
e. 选择*Enable*，然后查看要求列表。

f. 如果满足所有要求、请选择要使用的网格联合连接。

g. (可选)更改*复制删除标记*的设置，以确定S3客户端向不包含版本ID的源网格发出删除请求时目标网格上会发生什么情况：

▪ **Yes(默认)**：将删除标记添加到源存储分段并复制到目标存储分段。

▪ **否**：删除标记已添加到源存储分段，但不会复制到目标存储分段。



如果删除请求包含版本ID、则该对象版本将从源存储分段中永久删除。StorageGRID 不会复制包含版本ID的删除请求、因此不会从目标中删除相同的对象版本。

请参见 ["什么是跨网格复制"](#) 了解详细信息。

- a. (可选)更改*跨网格复制*审核类别的设置以管理审核消息的数量：
 - 错误(默认)：审核输出中仅包含失败的跨网格复制请求。
 - 正常：包括所有跨网格复制请求，这会显著增加审核输出的量。
- b. 查看您的选择。除非两个存储分段均为空、否则无法更改这些设置。
- c. 选择*启用并测试*。

片刻后、将显示一条成功消息。现在、添加到此存储分段的对象将自动复制到其他网格。*跨网格复制*在存储分段详细信息页面上显示为已启用的功能。

2. (可选)转至另一网格和上的相应存储分段 ["在两个方向上启用跨网格复制"](#)。

测试网格之间的复制

如果为存储分段启用了跨网格复制、则可能需要验证连接和跨网格复制是否正常工作、以及源存储分段和目标存储分段是否仍满足所有要求(例如、版本控制仍处于启用状态)。

开始之前

- 您正在使用 ["支持的 Web 浏览器"](#)。
- 您属于具有的用户组 ["root访问权限"](#)。

步骤

1. 登录到存储分段的租户帐户。
2. 从信息板中选择*查看存储分段*，或选择*存储(S3)*>*存储分段*。
3. 从表中选择存储分段名称以访问存储分段详细信息页面。
4. 选择*跨网格复制*选项卡。

5. 选择 * 测试连接 *。

如果连接运行状况良好、则会显示成功横幅。否则、将显示一条错误消息、您和网格管理员可以使用该消息来解析问题描述。有关详细信息，请参见 ["对网格联合错误进行故障排除"](#)。

6. 如果跨网格复制配置为双向进行，请转到另一网格上的相应分段，然后选择*测试连接*，以验证跨网格复制是否在另一个方向工作。

禁用跨网格复制

如果不再需要将对象复制到另一个网格、则可以永久停止跨网格复制。

禁用跨网格复制之前、请注意以下事项：

- 禁用跨网格复制不会删除已在网格之间复制的任何对象。例如、中的对象 `my-bucket` 在已复制到的网格1上 `my-bucket` 如果禁用了该存储分段的跨网格复制、则不会删除网格2上的。如果要删除这些对象、必须手动将其删除。
- 如果为每个分段启用了跨网格复制(即、如果是双向复制)、则可以为其中一个分段或这两个分段禁用跨网格复制。例如、您可能希望禁用从复制对象 `my-bucket` 在网格1上至 `my-bucket` 在网格2上、同时继续从复制对象 `my-bucket` 在网格2上至 `my-bucket` 在网格1上。
- 您必须先禁用跨网格复制、然后才能删除租户使用网格联盟连接的权限。请参见 ["管理允许的租户"](#)。
- 如果对包含对象的分段禁用跨网格复制、则无法重新启用跨网格复制、除非同时从源分段和目标分段中删除所有对象。



除非两个分段均为空、否则无法重新启用复制。

开始之前

- 您正在使用 ["支持的 Web 浏览器"](#)。
- 您属于具有的用户组 ["root访问权限"](#)。

步骤

1. 从不再需要复制对象的网格开始、停止对分段的跨网格复制：

- a. 登录到存储分段的租户帐户。
- b. 从信息板中选择*查看存储分段*，或选择*存储(S3)*>*存储分段*。
- c. 从表中选择存储分段名称以访问存储分段详细信息页面。
- d. 选择*跨网格复制*选项卡。
- e. 选择*禁用复制*。
- f. 如果确实要禁用此存储分段的跨网格复制，请在文本框中键入*Yes*，然后选择*Disable*。

片刻后、将显示一条成功消息。添加到此存储分段的新对象无法再自动复制到其他网格。*跨网格复制*不再显示为"分段"页面上的"已启用"功能。

2. 如果跨网格复制配置为双向进行、请转到另一个网格上的相应存储分段、并停止另一个方向的跨网格复制。

查看网格联合连接

如果您的租户帐户具有*使用网格联合连接*权限、则可以查看允许的连接。

开始之前

- 租户帐户具有*使用网格联合连接*权限。
- 您将使用登录到租户管理器 ["支持的 Web 浏览器"](#)。
- 您属于具有的用户组 ["root访问权限"](#)。

步骤

1. 选择*存储(S3)*>*网格联合连接*。

此时将显示"网格联合连接"页面、其中包含一个表、其中汇总了以下信息：

列	Description
连接名称	此租户有权使用的网格联盟连接。
具有跨网格复制的存储分段	对于每个网格联合连接、是指启用了跨网格复制的租户分段。添加到这些分段的对象将复制到连接中的其他网格。
上次错误	对于每个网格联合连接、在将数据复制到另一个网格时发生的最新错误(如果有)。请参见 清除上一个错误 。

2. (可选)为选择存储分段名称 ["查看存储分段详细信息"](#)。

清除上一个错误

由于以下原因之一，“上次错误”列中可能会出现错误：

- 未找到源对象版本。
- 未找到源存储分段。
- 已删除此目标存储分段。
- 目标存储分段已由其他帐户重新创建。
- 目标存储分段已暂停版本控制。
- 目标存储分段已由同一帐户重新创建、但现在已取消版本控制。



此列仅显示上次发生的跨网格复制错误；不会显示先前可能发生的错误。

步骤

1. 如果*last error*列中显示消息，请查看消息文本。

例如、此错误表示跨网格复制的目标分段处于无效状态、可能是因为版本控制已暂停或启用了S3对象锁定。

Grid federation connections

Clear error Search... Displaying one result

Connection name	Buckets with cross-grid replication	Last error
Grid 1-Grid 2	my-cgr-bucket	<p>2022-12-07 16:02:20 MST</p> <p>Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)</p>

2. 执行任何建议的操作。例如、如果在目标存储分段上暂停版本控制以进行跨网格复制、请为此存储分段重新启用版本控制。
3. 从表中选择连接。
4. 选择*清除错误*。
5. 选择*是*以清除消息并更新系统状态。
6. 等待5-6分钟、然后将新对象插入存储分段。确认错误信息不会再次出现。



要确保清除错误消息、请在消息中的时间戳后至少等待5分钟、然后再输入新对象。

7. 要确定是否有任何对象因存储分段错误而无法复制、请参见 ["确定并重试失败的复制操作"](#)。

版权信息

版权所有 © 2024 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。