使用租户帐户
StorageGRID

NetApp
November 04, 2025

目录

使用租户帐户

使用租户帐户：概述

租户帐户允许您使用简单存储服务（ S3 ） REST API 或 Swift REST API 在 StorageGRID 系统中存储和检索对象。

什么是租户帐户？

每个租户帐户都有自己的联合或本地组，用户， S3 分段或 Swift 容器以及对象。

租户帐户可用于按不同实体隔离存储的对象。例如，以下任一使用情形均可使用多个租户帐户：

- * 企业用例： * 如果在企业中使用 StorageGRID 系统，则网格的对象存储可能会被组织中的不同部门隔离。例如，可能存在营销部门，客户支持部门，人力资源部门等的租户帐户。

> 如果使用 S3 客户端协议，则还可以使用 S3 分段和分段策略在企业中的各个部门之间隔离对象。您无需创建单独的租户帐户。请参见实施说明 "S3存储分段和存储分段策略" 有关详细信息 …

- * 服务提供商用例： * 如果服务提供商正在使用 StorageGRID 系统，则网格的对象存储可能会被租用该存储的不同实体分隔。例如，可能存在公司 A ，公司 B ，公司 C 等的租户帐户。

如何创建租户帐户

租户帐户由创建 "使用网格管理器的 StorageGRID 网格管理员"。创建租户帐户时、网格管理员指定以下内容：

- 基本信息、包括租户名称、客户端类型(S3或Swift)和可选存储配额。
- 租户帐户的权限、例如租户帐户是否可以使用S3平台服务、配置自己的身份源、使用S3 Select或使用网格联盟连接。
- 租户的初始root访问权限、具体取决于StorageGRID 系统是使用本地组和用户、身份联合还是单点登录(SSO)。

此外，如果 S3 租户帐户需要符合法规要求，网格管理员可以为 StorageGRID 系统启用 S3 对象锁定设置。启用 S3 对象锁定后，所有 S3 租户帐户均可创建和管理合规的存储分段。

配置 **S3** 租户

在之后 "已创建 S3 租户帐户"，您可以访问租户管理器以执行以下任务：

- 设置身份联合(除非身份源与网格共享)
- 管理组和用户
- 使用网格联盟进行帐户克隆和跨网格复制
- 管理 S3 访问密钥
- 创建和管理S3存储分段

- 使用S3平台服务
- 使用 S3 Select
- 监控存储使用情况

虽然您可以使用租户管理器创建和管理S3存储分段、但必须使用S3客户端来加存和管理对象。请参见 "使用S3 REST API" 了解详细信息。

配置 **Swift** 租户

在 A 之后 "已创建 Swift 租户帐户"，您可以访问租户管理器以执行以下任务：

- 设置身份联合(除非身份源与网格共享)
- 管理组和用户
- 监控存储使用情况

Swift 用户必须具有 root 访问权限才能访问租户管理器。但是、root访问权限不允许用户在中进行身份验证 "Swift REST API" 创建容器和载入对象。用户必须具有 Swift 管理员权限才能向 Swift REST API 进行身份验证。

如何登录和注销

登录到租户管理器

您可以通过在的地址栏中输入租户的 URL 来访问租户管理器 "支持的 Web 浏览器"。

开始之前

- 您已拥有登录凭据。
- 网格管理员提供了一个用于访问租户管理器的URL。URL 将类似于以下示例之一：

```
https://FQDN_or_Admin_Node_IP/

https://FQDN_or_Admin_Node_IP:port/

https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

此URL始终包括完全限定域名(FQDN)、管理节点的IP地址或管理节点HA组的虚拟IP地址。它可能还包括端口号、20位租户帐户ID或这两者。

- 如果URL不包括租户的20位帐户ID、则您具有此帐户ID。
- 您正在使用 "支持的 Web 浏览器"。
- 已在 Web 浏览器中启用 Cookie 。
- 您属于具有的用户组 "特定访问权限"。

步骤

1. 启动 "支持的 Web 浏览器"。
2. 在浏览器的地址栏中，输入用于访问租户管理器的 URL 。
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。
4. 登录到租户管理器。

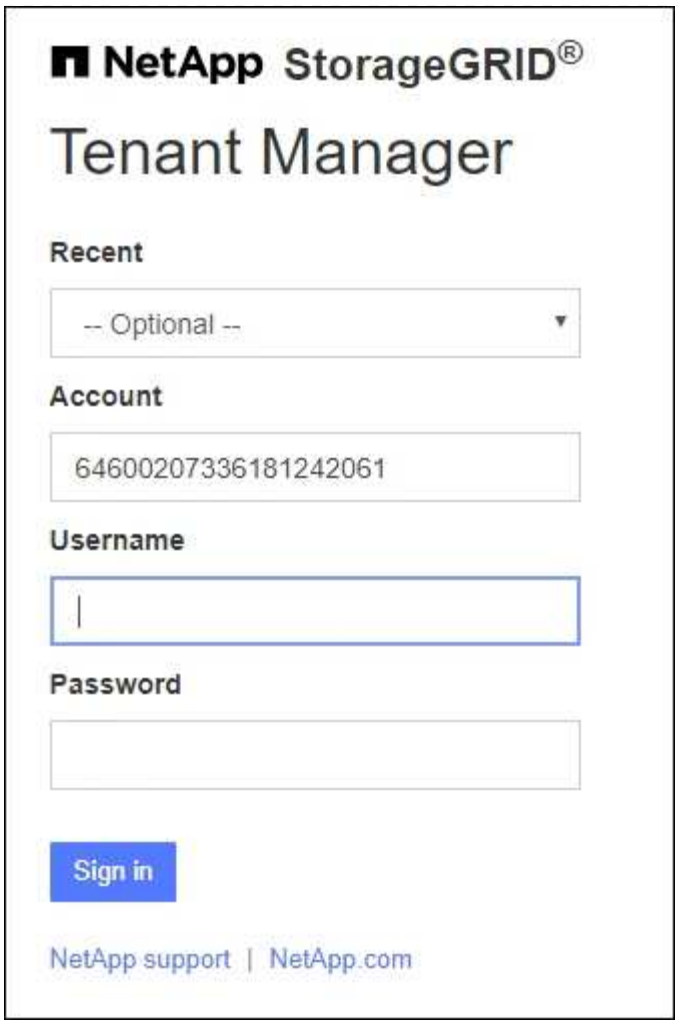
   显示的登录屏幕取决于您输入的URL以及是否已为StorageGRID 配置单点登录(Single Sign On、SSO)。

未使用**SSO**

如果StorageGRID 未使用SSO、则会显示以下屏幕之一：

- 网格管理器登录页面。选择*租户登录*链接。

- 租户管理器登录页面。“帐户”字段可能已完成，如下所示。



i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。

ii. 输入用户名和密码。

iii. 选择 * 登录 * 。

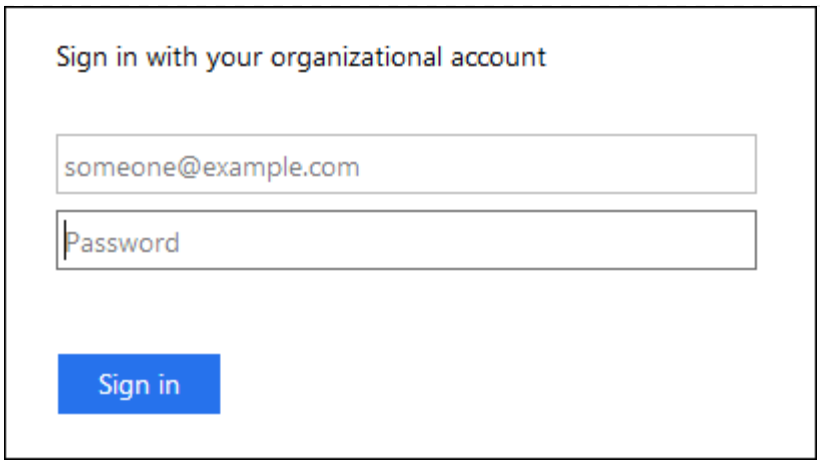
此时将显示租户管理器信息板。

iv. 如果您收到了其他人的初始密码，请选择*_USERNAME_*>*更改密码*以保护您的帐户。

使用**SSO**

如果StorageGRID 正在使用SSO、则会显示以下屏幕之一：

- 您组织的SSO页面。例如：



输入您的标准SSO凭据，然后选择*登录*。

- 租户管理器 SSO 登录页面。

i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。

ii. 选择 * 登录 * 。

iii. 在您组织的 SSO 登录页面上使用您的标准 SSO 凭据登录。

此时将显示租户管理器信息板。

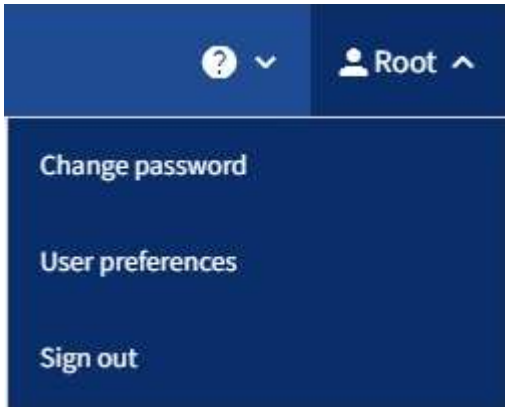
注销租户管理器

使用租户管理器完成操作后、您必须注销以确保未经授权的用户无法访问StorageGRID 系

统。根据浏览器 Cookie 设置，关闭浏览器可能无法将您从系统中注销。

步骤

1. 找到用户界面右上角的用户名下拉列表。



2. 选择用户名，然后选择*Sign Out。

   - 如果未使用 SSO：

     您已从管理节点注销。此时将显示租户管理器登录页面。

     如果您已登录到多个管理节点，则必须从每个节点注销。

   - 如果启用了 SSO：

     您已从正在访问的所有管理节点中注销。此时将显示 StorageGRID 登录页面。您刚刚访问的租户帐户的名称将在 * 近期帐户 * 下拉列表中列为默认名称，并显示租户的 * 帐户 ID* 。

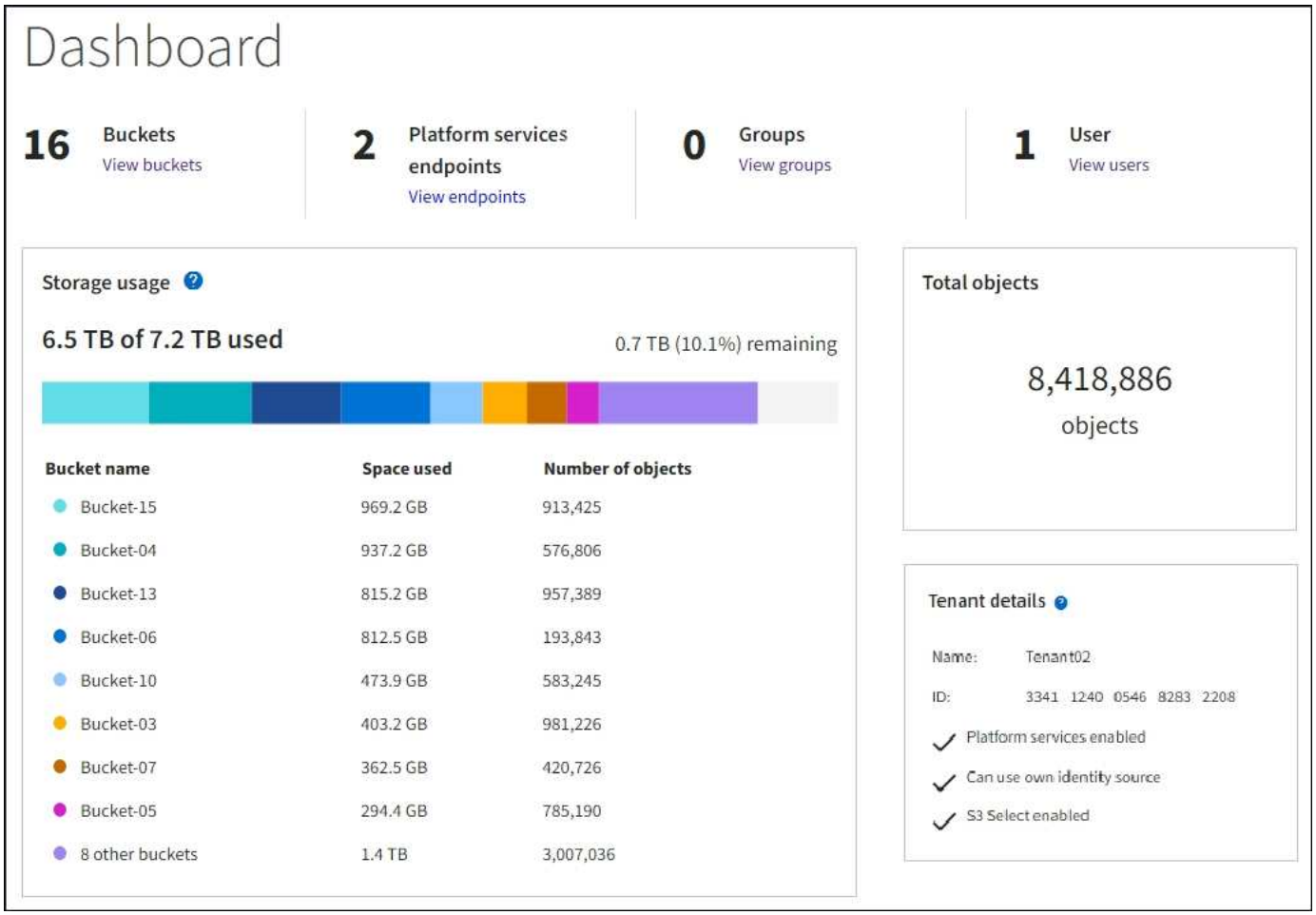
如果启用了 SSO ，并且您还登录到网格管理器，则还必须注销网格管理器才能注销 SSO 。

了解租户管理器信息板

租户管理器信息板简要介绍租户帐户的配置以及租户分段(S3)或容器(Swift)中的对象使用的空间量。如果租户具有配额、则此信息板将显示已使用的配额量以及剩余的配额量。如果存在与租户帐户相关的任何错误、这些错误将显示在信息板上。

" 已用空间 " 值是估计值。这些估计值受载入时间，网络连接和节点状态的影响。

上载对象后、信息板将类似于以下示例：



租户帐户摘要

信息板顶部包含以下信息：

- 已配置的分段或容器，组和用户的数量
- 已配置的平台服务端点数量（如果有）

您可以选择这些链接来查看详细信息。

信息板右侧包含以下信息：

- 租户的对象总数。

  对于S3帐户、如果尚未载入任何对象、并且您具有root访问权限、则会显示Getting Started (入门)准则、而不是对象总数。

- 租户详细信息，包括租户帐户名称和 ID 以及租户是否可以使用 "平台服务"， "自己的身份源"， "网格联盟" 或 "S3 Select" （仅列出已启用的权限）。

存储和配额使用量

存储使用情况面板包含以下信息：

- 租户的对象数据量。

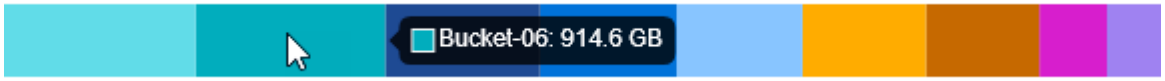
此值表示已上传的对象数据总量，不表示用于存储这些对象及其元数据副本的空间。

- 如果设置了配额，则表示可用于对象数据的总空间量以及剩余空间量和百分比。配额限制了可载入的对象数据量。

配额使用量基于内部估计值、在某些情况下可能会超过此值。例如，当租户开始上传对象时， StorageGRID 会检查配额，如果租户超过配额，则会拒绝新的载入。但是，在确定是否超过配额时， StorageGRID 不会考虑当前上传的大小。如果删除了对象、则可能会暂时阻止租户上传新对象、直到重新计算配额使用量为止。计算配额使用量可能需要10分钟或更长时间。

- 一个条形图，表示最大分段或容器的相对大小。

  您可以将光标置于任何图表区块上方，以查看该分段或容器占用的总空间。



- 要与条形图相对应，需要列出最大的分段或容器，包括对象数据总量以及每个分段或容器的对象数量。

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

如果租户具有九个以上的分段或容器，则所有其他分段或容器将合并到列表底部的一个条目中。

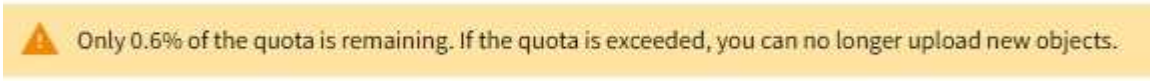
要更改租户管理器中显示的存储值的单位、请选择租户管理器右上角的用户下拉列表、然后选择*用户首选项*。

配额使用情况警报

如果已在网格管理器中启用配额使用情况警报，则在配额不足或超过配额时，这些警报将显示在租户管理器中，

如下所示：

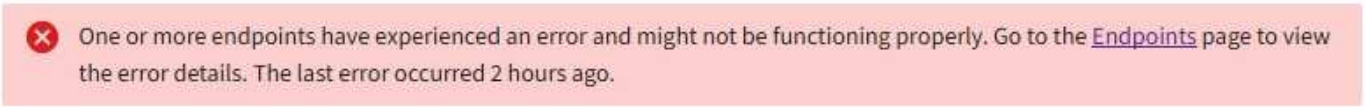
如果已使用租户配额的 90% 或更多，则会触发 * 租户配额使用量高 * 警报。对警报执行建议的操作。



如果超过配额、则无法上传新对象。

端点错误

如果已使用网格管理器配置一个或多个端点以用于平台服务、则租户管理器信息板会在过去七天内发生任何端点错误时显示警报。



以查看有关的详细信息 "平台服务端点错误"下，选择*end点*以显示端点页面。

租户管理 API

了解租户管理 API

您可以使用租户管理 REST API 执行系统管理任务，而不是使用租户管理器用户界面。例如，您可能希望使用 API 来自动执行操作或更快地创建多个实体，例如用户。

租户管理 API ：

- 使用 Swagger 开源 API 平台。Swagger 提供了一个直观的用户界面，支持开发人员和非开发人员与 API 进行交互。Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。
- 用途 "版本控制以支持无中断升级"。

要访问租户管理 API 的 Swagger 文档，请执行以下操作：

1. 登录到租户管理器。
2. 从租户管理器的顶部、选择帮助图标并选择* API文档*。

API 操作

租户管理 API 将可用的 API 操作组织到以下部分中：

- 帐户：对当前租户帐户执行的操作、包括获取存储使用情况信息。
- **auth**：执行用户会话身份验证的操作。

租户管理 API 支持不承载令牌身份验证方案。对于租户登录、您可以在身份验证请求的JSON正文中提供用户名、密码和帐户ID (即、 `POST /api/v3/authorize`）。如果用户已成功通过身份验证，则会返回一个安全令牌。此令牌必须在后续 API 请求的标题中提供（ " 授权：承载令牌 " ）。

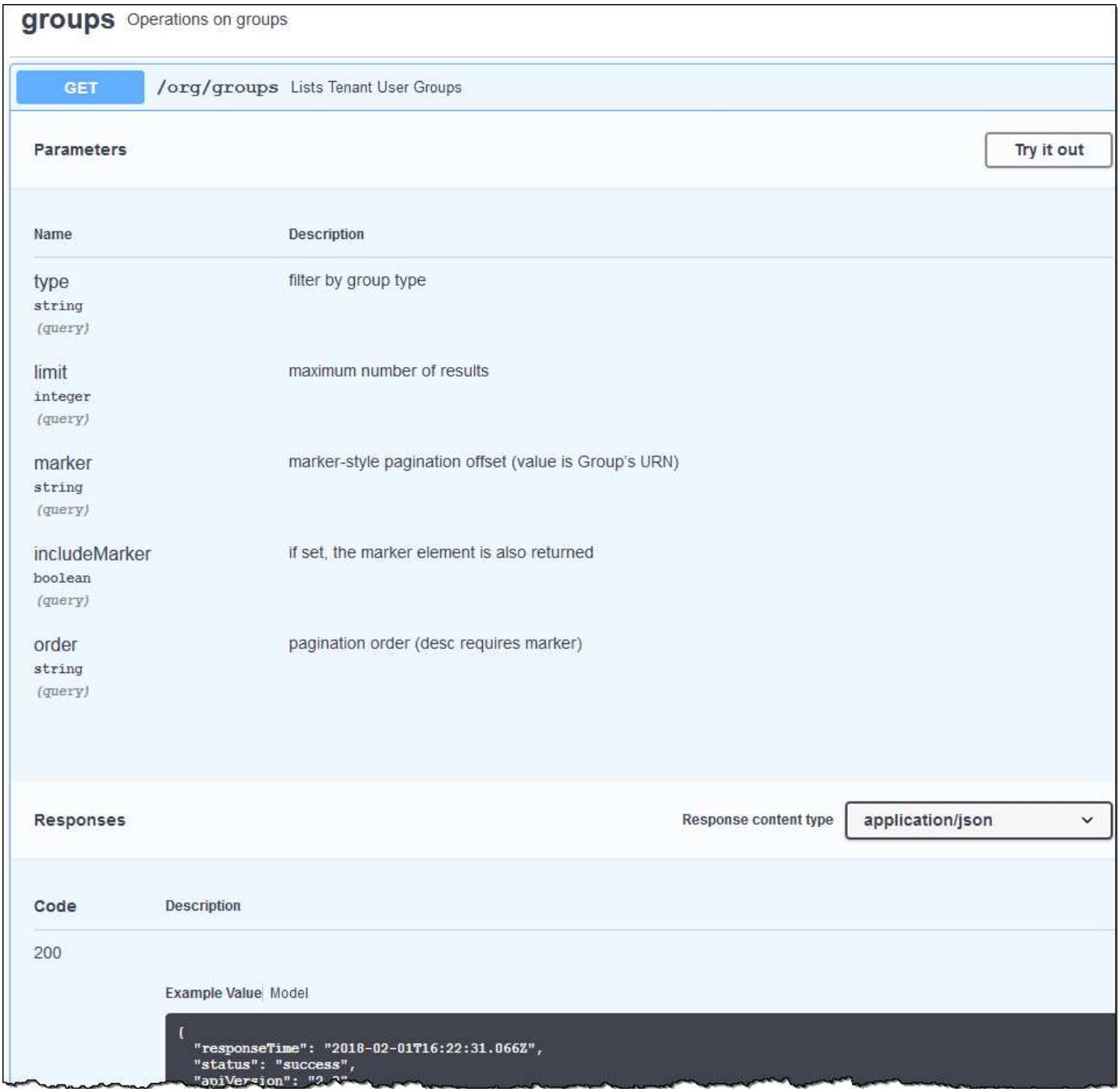
有关提高身份验证安全性的信息，请参见 "防止跨站点请求伪造"。

> 如果为 StorageGRID 系统启用了单点登录（ SSO ），则必须执行不同的步骤进行身份验证。请参见 "有关使用网格管理 API 的说明"。

- **config**：与租户管理API的产品版本和版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- 容器：对S3存储分段或Swift容器执行操作。
- *DEactive-Features *：用于查看可能已停用的功能的操作。
- 端点：用于管理端点的操作。通过端点， S3 存储分段可以使用外部服务进行 StorageGRID CloudMirror 复制，通知或搜索集成。
- 网格联合连接：对网格联合连接和跨网格复制的操作。
- 组：用于管理本地租户组和从外部身份源检索联合租户组的操作。
- 身份源：用于配置外部身份源以及手动同步联盟组和用户信息的操作。
- 区域：用于确定已为StorageGRID 系统配置了哪些区域的操作。
- **S3**：用于管理租户用户的S3访问密钥的操作。
- **S3-object-lock**：对全局S3对象锁定设置执行操作，用于支持合规性。
- 用户：用于查看和管理租户用户的操作。

操作详细信息

展开每个 API 操作时，您可以看到其 HTTP 操作，端点 URL ，任何必需或可选参数的列表，请求正文示例（如果需要）以及可能的响应。



问题描述 **API** 请求

使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

步骤

1. 选择 HTTP 操作以查看请求详细信息。
2. 确定此请求是否需要其他参数，例如组或用户 ID 。然后，获取这些值。您可能需要先对其他 API 请求进行问题描述 处理，以获取所需的信息。
3. 确定是否需要修改示例请求正文。如果是，您可以选择 * 型号 * 来了解每个字段的要求。
4. 选择 * 试用 * 。

5. 提供所需的任何参数，或根据需要修改请求正文。
6. 选择 * 执行 * 。
7. 查看响应代码以确定请求是否成功。

租户管理 API 版本控制

租户管理 API 使用版本控制来支持无中断升级。

例如，此请求 URL 指定 API 版本 3 。

`https://hostname_or_ip_address/api/v3/authorize`

如果所做的更改与旧版本"不兼容"、则租户管理API的主要版本会发生碰撞。如果对_are compender_与旧版本进行了更改、则租户管理API的次要版本会发生碰撞。兼容的更改包括添加新端点或新属性。以下示例说明了如何根据所做更改的类型对 API 版本进行递增。

API 的更改类型	旧版本	新版本
与旧版本兼容	2.1	2.2
与旧版本不兼容	2.1	3.0

首次安装 StorageGRID 软件时，仅会启用最新版本的租户管理 API 。但是，在将 StorageGRID 升级到新功能版本后，您仍可访问至少一个 StorageGRID 功能版本的旧版 API 。

已过时的请求将通过以下方式标记为已弃用：

- 响应标头为 "depression: true"
- JSON 响应正文包含 "depressioned" ： true

确定当前版本支持哪些 API 版本

请使用以下 API 请求返回受支持的 API 主要版本列表：

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

指定请求的 **API** 版本

您可以使用path参数指定API版本 (`/api/v3`)或标题 (`Api-Version: 3`）。如果同时提供这两个值，则标头值将覆盖路径值。

```
curl https://<IP-Address>/api/v3/grid/accounts
```

```
curl -H "Api-Version: 3" https://<IP-Address>/api/grid/accounts
```

防止跨站点请求伪造（ **CSRF** ）

您可以通过使用 CSRF 令牌增强使用 Cookie 的身份验证，帮助防止 StorageGRID 受到跨站点请求伪造（ CSRF ）攻击。网格管理器和租户管理器会自动启用此安全功能；其他 API 客户端可以选择在登录时是否启用此功能。

如果攻击者可能触发对其他站点的请求（例如使用 HTTP 表单发布），则可以对使用已登录用户的 cookie 发出的某些请求进行发生原因 处理。

StorageGRID 可通过使用 CSRF 令牌帮助防止 CSRF 攻击。启用后，特定 Cookie 的内容必须与特定标题或特定后处理正文参数的内容匹配。

要启用此功能、请设置 `csrfToken` 参数设置为 `true` 身份验证期间。默认值为 `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果为true、则为A `GridCsrfToken` Cookie会使用随机值设置为网格管理器和登录 `AccountCsrfToken` Cookie会使用随机值设置为登录到租户管理器。

如果存在 Cookie ，则可以修改系统状态的所有请求（ POST ， PUT ， patch ， delete ）都必须包括以下项之一：

- 。 `X-Csrf-Token` 标头、标头的值设置为CSRF令牌cookie的值。
- 对于接受表单编码正文的端点：A `csrfToken` 表单编码的请求正文参数。

要配置 CSRF 保护，请使用 "网格管理 API" 或 "租户管理 API"。

> 设置了CSRF令牌Cookie的请求也将强制实施 `"Content-Type: application/json"` 任何请求的标头、如果希望JSON请求正文作为对CSRF攻击的额外保护、

使用网格联合连接

克隆租户组和用户

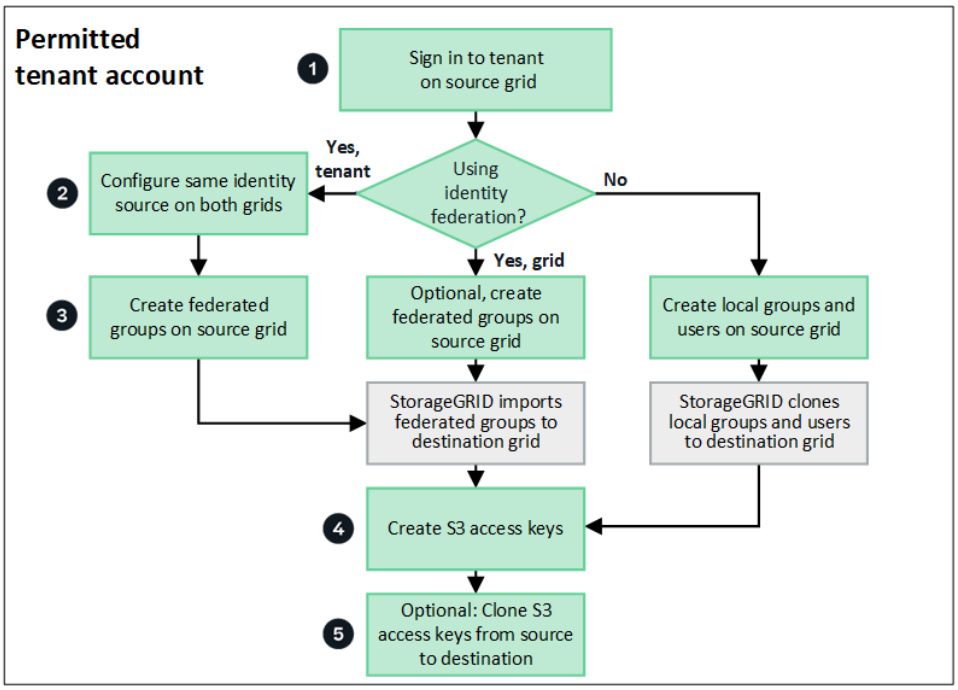
如果新租户有权使用网格联合连接、则在创建该租户时、该租户会从一个StorageGRID 系统复制到另一个StorageGRID 系统。复制租户后、添加到源租户的任何组和用户将克隆到目标租户。

最初创建租户的StorageGRID 系统是租户的_ssource 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*权限来使用联盟组和用户、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 创建组和用户

创建组和用户时、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 系统或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" 在源网格或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"。

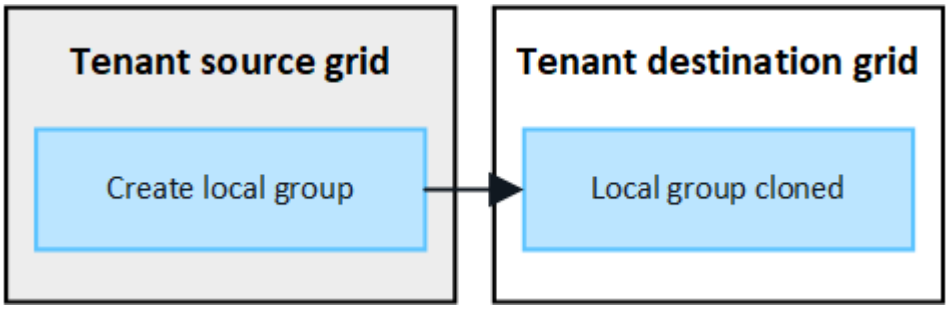
如何克隆组、用户和**S3**访问密钥?

查看本节、了解如何在租户源网格和租户目标网格之间克隆组、用户和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、组权限和S3组策略。有关说明，请参见 "为 S3 租户创建组"。

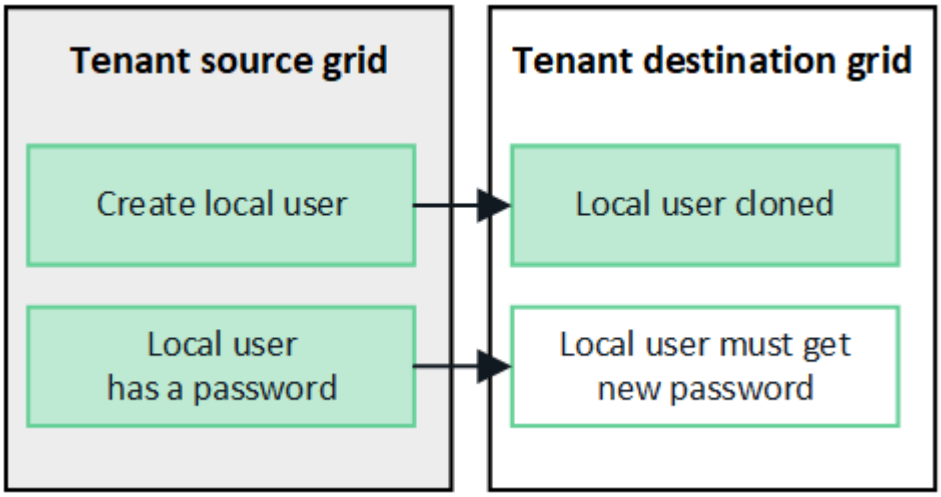


> 在源网格上创建本地组时选择的任何用户、在将组克隆到目标网格时均不包括在内。因此、请勿在创建组时选择用户。而是在创建用户时选择组。

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、用户名和*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"。

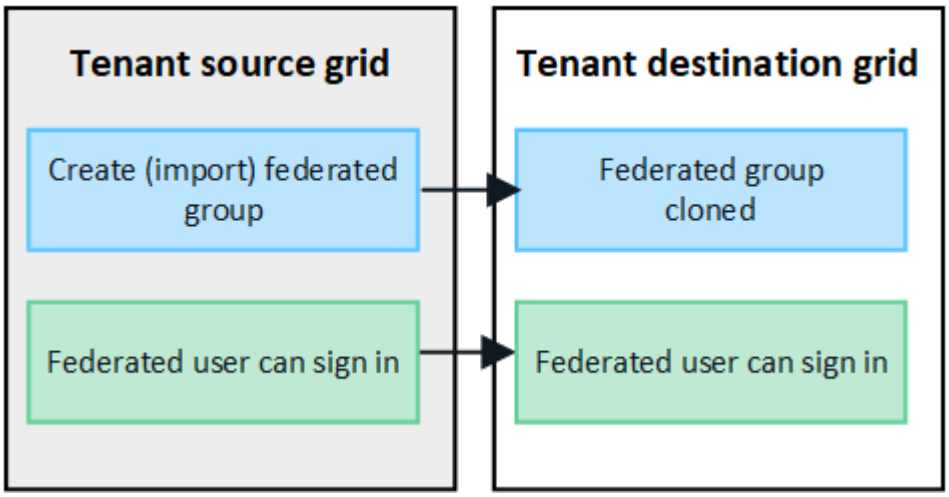


克隆在源网格上创建的联盟组

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。

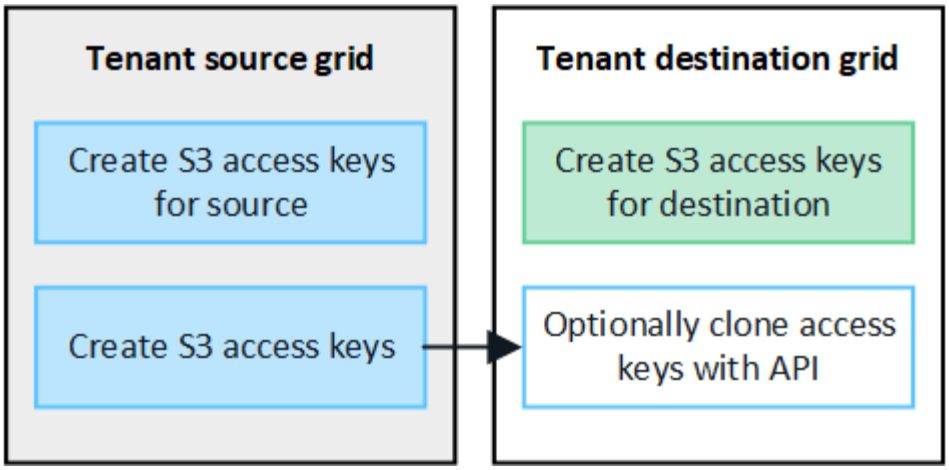


可以手动克隆**S3**访问密钥

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：

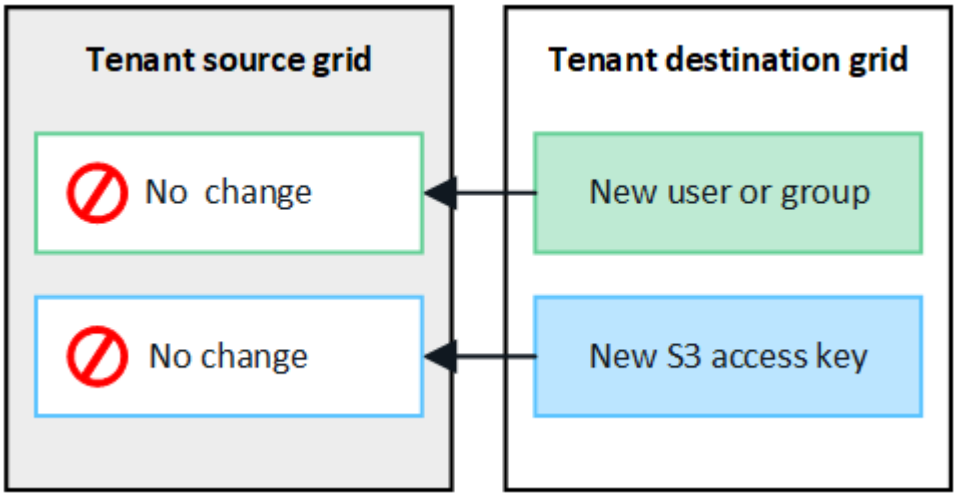
- 如果您不需要对每个网格使用相同的键、则可以使用 "创建您自己的访问密钥" 或 "创建其他用户的访问密钥" 在每个网格上。
- 如果需要在两个网格上使用相同的密钥、可以在源网格上创建密钥、然后使用租户管理器API手动创建 "克隆密钥" 到目标网格。



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

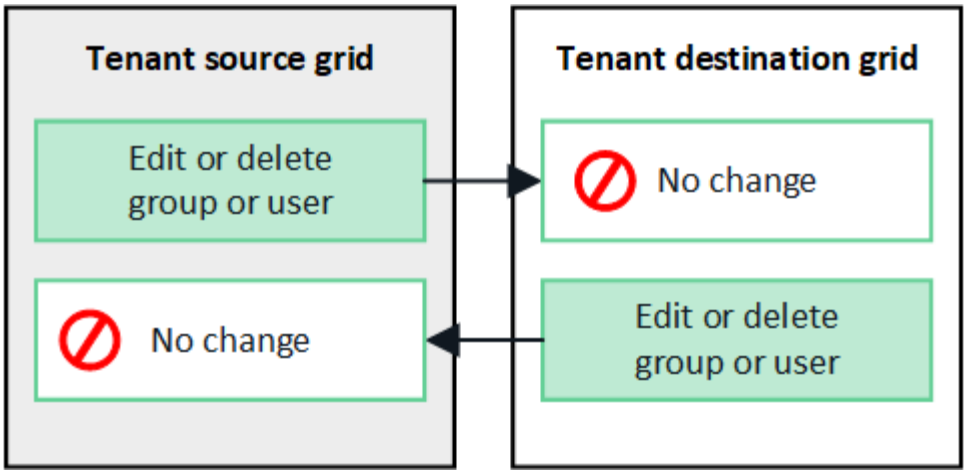
只会从租户的源网格克隆到租户的目标网格。如果在租户的目标网格上创建或导入组和用户、StorageGRID 不会将这些项克隆回租户的源网格。



编辑或删除的组、用户和访问密钥不会克隆

只有在创建新组和用户时、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。

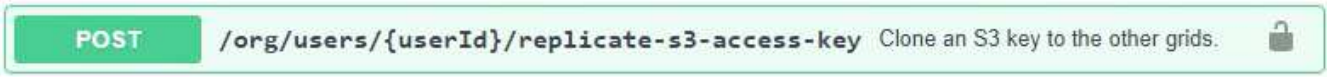
步骤

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)。

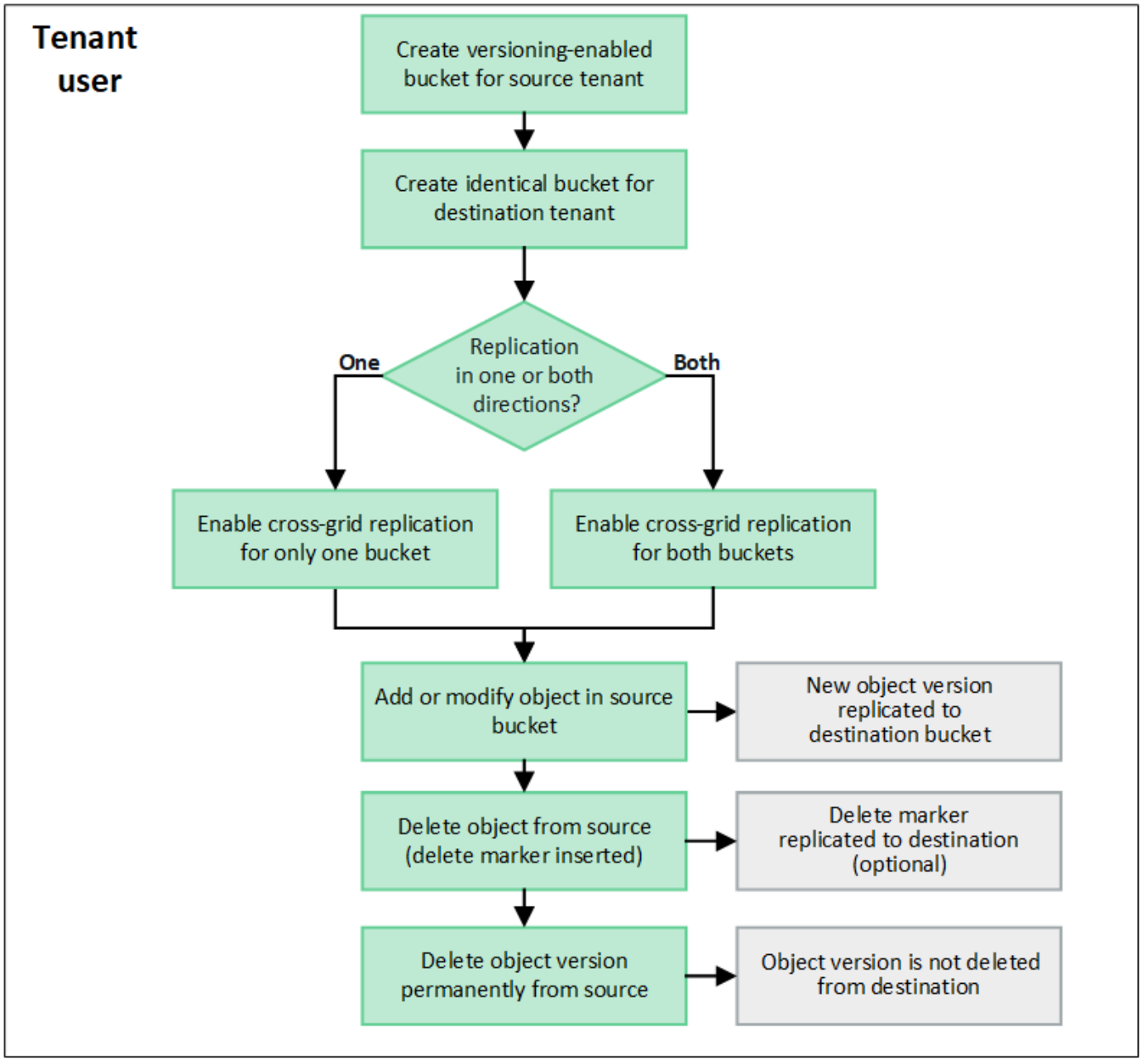
9. 选择 * 执行 * 。
10. 确认服务器响应代码为*204*，表示密钥已成功克隆到目标网格。

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。

跨网格复制工作流

此工作流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。

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。

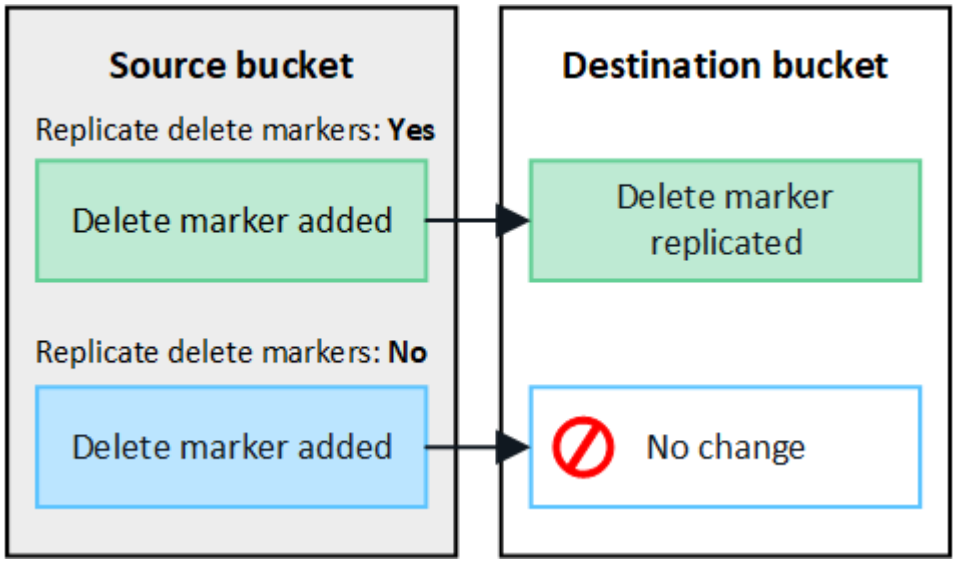
步骤

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：

- 如果*Yes*(默认值)，则会将删除标记添加到源存储分段并复制到目标存储分段。
- 如果*否*，删除标记将添加到源存储分段，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. 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。

b. 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。

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"。

管理组和用户

使用身份联合

使用身份联合可以加快租户组和用户的设置速度，并允许租户用户使用熟悉的凭据登录到租户帐户。

为租户管理器配置身份联合

如果您希望在 Active Directory ， Azure Active Directory （ Azure AD ）， OpenLDAP 或 Oracle Directory Server 等其他系统中管理租户组和用户，则可以为租户管理器配置身份联合。

开始之前

- 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"。
- 您正在使用 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

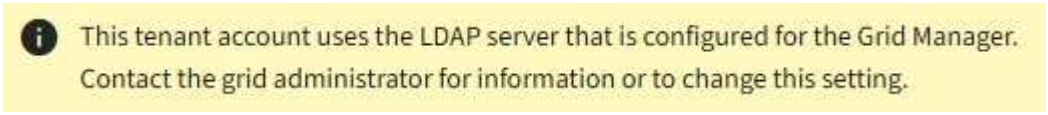
> 如果要使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP ，则必须配置 OpenLDAP 服务器。请参见 配置 OpenLDAP 服务器的准则。
- 如果您计划使用传输层安全（ Transport Layer Security ， TLS ）与 LDAP 服务器进行通信，则身份提供程

序必须使用 TLS 1.2 或 1.3 。请参见 "支持传出 TLS 连接的密码"。

关于此任务

是否可以为租户配置身份联合服务取决于租户帐户的设置方式。您的租户可能会共享为网格管理器配置的身份联合服务。如果在访问"身份联合"页面时看到此消息、则无法为此租户配置单独的联合身份源。

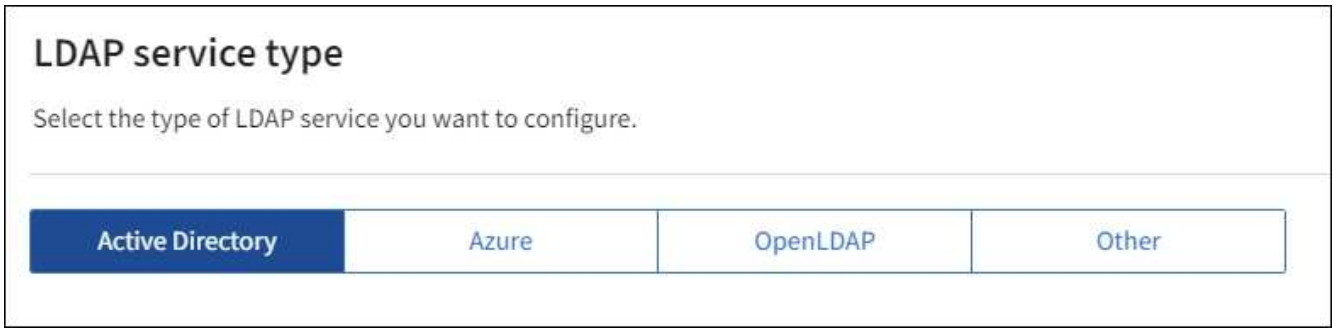


进入配置

在配置"标识联盟"时、您可以提供StorageGRID 连接到LDAP服务所需的值。

步骤

1. 选择 * 访问管理 * > * 身份联合 * 。
2. 选择 * 启用身份联合 * 。
3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。



选择 * 其他 * 可为使用 Oracle 目录服务器的 LDAP 服务器配置值。

4. 如果选择了 * 其他 * ，请填写 LDAP 属性部分中的字段。否则，请继续执行下一步。
   - * 用户唯一名称 * ： 包含 LDAP 用户唯一标识符的属性的名称。此属性等效于 `sAMAccountName` 适用于Active Directory和 `uid` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `uid`。
   - * 用户 UID* ： 包含 LDAP 用户的永久唯一标识符的属性的名称。此属性等效于 `objectGUID` 适用于Active Directory和 `entryUUID` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `nsuniqueid`。每个用户在指定属性中的值都必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
   - * 组唯一名称 * ： 包含 LDAP 组唯一标识符的属性的名称。此属性等效于 `sAMAccountName` 适用于Active Directory和 `cn` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `cn`。
   - * 组 UID* ： 包含 LDAP 组的永久唯一标识符的属性的名称。此属性等效于 `objectGUID` 适用于Active Directory和 `entryUUID` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `nsuniqueid`。每个组在指定属性中的值必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
5. 对于所有 LDAP 服务类型，请在配置 LDAP 服务器部分中输入所需的 LDAP 服务器和网络连接信息。
   - * 主机名 * ： LDAP 服务器的完全限定域名（ FQDN ）或 IP 地址。
   - * 端口 * ： 用于连接到 LDAP 服务器的端口。

STARTTLS 的默认端口为 389 ， LDAPS 的默认端口为 636 。但是，只要防火墙配置正确，您就可以使用任何端口。

- * 用户名 * ：要连接到 LDAP 服务器的用户的可分辨名称（ DN ）的完整路径。

  对于 Active Directory ，您还可以指定低级别的登录名称或用户主体名称。

  指定的用户必须具有列出组和用户以及访问以下属性的权限：

  - `sAMAccountName` 或 `uid`
  - `objectGUID`， `entryUUID`或 `nsuniqueid`
  - `cn`
  - `memberOf` 或 `isMemberOf`
  - **Active Directory**： `objectSid`， `primaryGroupID`， `userAccountControl`，和 `userPrincipalName`
  - * Azure *： `accountEnabled` 和 `userPrincipalName`

- * 密码 * ：与用户名关联的密码。
- * 组基本 DN* ：要搜索组的 LDAP 子树的可分辨名称（ DN ）的完整路径。在 Active Directory 示例（如下）中，可分辨名称相对于基础 DN （ DC=storagegrid ， DC=example ， DC=com ）的所有组均可用作联合组。

  * 组唯一名称 * 值在其所属的 * 组基本 DN* 中必须是唯一的。

- * 用户基础 DN* ：要搜索用户的 LDAP 子树的可分辨名称（ DN ）的完整路径。

  用户唯一名称 * 值在其所属的 * 用户基础 DN* 中必须是唯一的。

- 绑定用户名格式(可选)：如果无法自动确定模式，StorageGRID 应使用默认用户名模式。

  建议提供 * 绑定用户名格式 * ，因为如果 StorageGRID 无法绑定到服务帐户，它可以允许用户登录。

  输入以下模式之一：

  - **UserPrincipalName模式(Active Directory和Azure)**： `[USERNAME]@example.com`
  - 低级登录名称模式**(Active Directory和Azure)**： `example\[USERNAME]`
  - 可分辨名称模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。
   - * 使用 STARTTLS * ：使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是建议的 Active Directory ， OpenLDAP 或其他选项，但 Azure 不支持此选项。
   - * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。您必须为 Azure 选择此选项。

- * 请勿使用 TLS* ： StorageGRID 系统与 LDAP 服务器之间的网络流量将不会受到保护。Azure 不支持此选项。

> 如果 Active Directory 服务器强制实施 LDAP 签名，则不支持使用 * 不使用 TLS* 选项。您必须使用 STARTTLS 或 LDAPS 。

7. 如果选择 STARTTLS 或 LDAPS ，请选择用于保护连接安全的证书。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认网格 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义安全证书。

     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

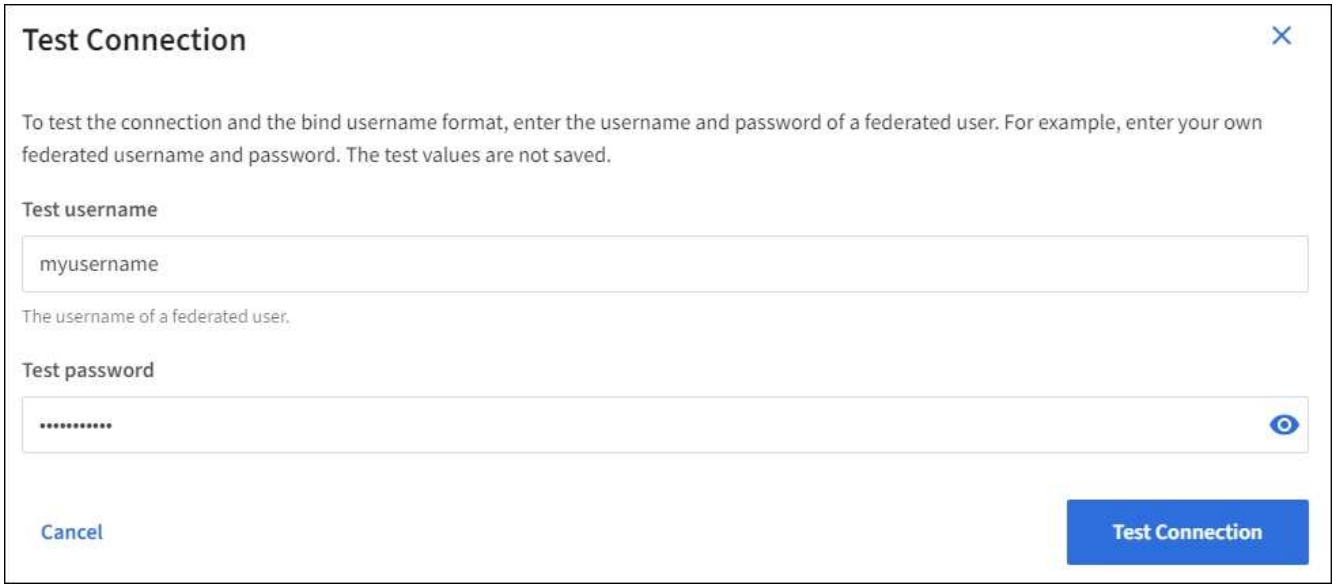
测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。如果您提供了 LDAP 服务器的连接设置和绑定用户名格式，则 StorageGRID 会对其进行验证。

步骤

1. 选择 * 测试连接 * 。
2. 如果未提供绑定用户名格式：
   - 如果连接设置有效，则会显示 "`Test connection successful` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置无效，则会显示 "`test connection could not be established` " 消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。
3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

   例如，输入您自己的用户名和密码。请勿在用户名中包含任何特殊字符、例如@或/。



   - 如果连接设置有效，则会显示 "`Test connection successful` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置，绑定用户名格式或测试用户名和密码无效，则会显示一条错误消息。解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统会定期同步身份源中的联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到身份联合页面。
2. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

   如果存在正在同步身份源中的联合组和用户的问题描述 ，则会触发 * 身份联合同步失败 * 警报。

禁用身份联合

您可以临时或永久禁用组和用户的身份联合。禁用身份联合后， StorageGRID 与身份源之间不会进行通信。但是，您配置的任何设置都将保留下来，以便将来可以轻松地重新启用身份联合。

关于此任务

在禁用身份联合之前，您应注意以下事项：

- 联合用户将无法登录。
- 当前已登录的联合用户将保留对 StorageGRID 系统的访问权限，直到其会话到期为止，但在其会话到期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，并且不会为尚未同步的帐户发出警报或警报。
- 如果单点登录(SSO)设置为*Enabled"或*Sandbox Mode*，则*启用身份联合*复选框将被禁用。在禁用身份联合之前，单点登录页面上的 SSO 状态必须为 * 已禁用 * 。请参见 "禁用单点登录"。

步骤

1. 转到身份联合页面。
2. 取消选中*启用身份联合*复选框。

配置 **OpenLDAP** 服务器的准则

如果要使用 OpenLDAP 服务器进行身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

对于非ActiveDirectory或Azure身份源、StorageGRID 不会自动阻止外部禁用的用户进行S3访问。要阻止S3访问、请删除此用户的任何S3密钥或从所有组中删除此用户。

memberOf 和 **fint** 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

索引编制

您必须使用指定的索引关键字配置以下 OpenLDAP 属性：

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

此外，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

管理租户组

为 **S3** 租户创建组

您可以通过导入联合组或创建本地组来管理 S3 用户组的权限。

开始之前

- 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"。
- 如果您计划导入联盟组、则需要 "已配置身份联合"，并且已配置的身份源中已存在联盟组。
- 如果您的租户帐户具有*使用网格联合连接*权限、则您已查看的工作流和注意事项 "克隆租户组和用户"，您将登录到租户的源网格。

访问创建组向导

首先、访问创建组向导。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 如果您的租户帐户具有*使用网格联合连接*权限、请确认显示蓝色横幅、指示在此网格上创建的新组将克隆到连接中另一网格上的同一租户。如果未显示此横幅、则您可能已登录到租户的目标网格。

3. 选择 * 创建组 * 。

选择组类型

您可以创建本地组或导入联合组。

步骤

1. 选择 * 本地组 * 选项卡以创建本地组，或者选择 * 联合组 * 选项卡以从先前配置的身份源导入组。

   如果为 StorageGRID 系统启用了单点登录（ SSO ），则属于本地组的用户将无法登录到租户管理器，但他们可以根据组权限使用客户端应用程序管理租户的资源。

2. 输入组的名称。
   - * 本地组 * ： 输入显示名称和唯一名称。您可以稍后编辑显示名称。

     如果您的租户帐户具有*使用网格联合连接*权限、并且目标网格上的租户已存在相同的*唯一名称*、则会发生克隆错误。

   - * 联合组 * ： 输入唯一名称。对于Active Directory、唯一名称是与关联的名称 `sAMAccountName` 属性。对于OpenLDAP、唯一名称是与关联的名称 `uid` 属性。
3. 选择 * 继续 * 。

管理组权限

组权限控制用户可在租户管理器和租户管理API中执行的任务。

步骤

1. 对于*Access mode*，请选择以下选项之一：
   - 读写(默认)：用户可以登录到租户管理器并管理租户配置。
   - * 只读 * ： 用户只能查看设置和功能。他们无法在租户管理器或租户管理API中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。

     如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。

2. 为此组选择一个或多个权限。

   请参见 "租户管理权限"。

3. 选择 * 继续 * 。

设置S3组策略

组策略用于确定用户将拥有哪些S3访问权限。

步骤

1. 选择要用于此组的策略。

组策略	Description
无S3访问	默认。此组中的用户无权访问S3资源、除非使用存储分段策略授予访问权限。如果选择此选项，则默认情况下，只有 root 用户才能访问 S3 资源。
只读访问	此组中的用户对S3资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。选择此选项后，只读组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
完全访问	此组中的用户对S3资源(包括分段)具有完全访问权限。选择此选项后，完全访问组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
勒索软件防护	此示例策略适用场景 all分段for this租户。此组中的用户可以执行常见操作、但无法从启用了对象版本控制的分段中永久删除对象。 具有*管理所有存储分段*权限的租户管理器用户可以覆盖此组策略。将"管理所有分段"权限限制为受信任用户、并在可用时使用多因素身份验证(Multi-FactorAuthentication、MFA)。
自定义	组中的用户将被授予您在文本框中指定的权限。

2. 如果选择 * 自定义 * ，请输入组策略。每个组策略的大小限制为 5 ， 120 字节。您必须输入有效的 JSON 格式字符串。

   有关组策略的详细信息、包括语言语法和示例、请参见 "组策略示例"。

3. 如果要创建本地组，请选择 * 继续 * 。如果要创建联合组，请选择 * 创建组 * 和 * 完成 * 。

添加用户（仅限本地组）

您可以保存组而不添加用户、也可以选择添加任何已存在的本地用户。

> 如果您的租户帐户具有*使用网格联合连接*权限、则在源网格上创建本地组时选择的任何用户在克隆到目标网格时不会包括在其中。因此、请勿在创建组时选择用户。而是在创建用户时选择组。

步骤

1. 或者，为此组选择一个或多个本地用户。
2. 选择 * 创建组 * 和 * 完成 * 。

   您创建的组将显示在组列表中。

   如果您的租户帐户具有*使用网格联合连接*权限、而您位于租户的源网格上、则新组将克隆到租户的目标网格。成功*显示为组详细信息页面的"概述"部分中的*克隆状态。

为 **Swift** 租户创建组

您可以通过导入联合组或创建本地组来管理 Swift 租户帐户的访问权限。至少有一个组必须具有 Swift 管理员权限，这是管理 Swift 租户帐户的容器和对象所必需的。

对Swift客户端应用程序的支持已弃用、将在未来版本中删除。

开始之前

- 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"。
- 如果您计划导入联盟组、则需要 "已配置身份联合"，并且已配置的身份源中已存在联盟组。

访问创建组向导

步骤

首先、访问创建组向导。

1. 选择 * 访问管理 * > * 组 * 。
2. 选择 * 创建组 * 。

选择组类型

您可以创建本地组或导入联合组。

步骤

1. 选择 * 本地组 * 选项卡以创建本地组，或者选择 * 联合组 * 选项卡以从先前配置的身份源导入组。

   如果为 StorageGRID 系统启用了单点登录（ SSO ），则属于本地组的用户将无法登录到租户管理器，但他们可以根据组权限使用客户端应用程序管理租户的资源。

2. 输入组的名称。
   - * 本地组 * ： 输入显示名称和唯一名称。您可以稍后编辑显示名称。
   - * 联合组 * ： 输入唯一名称。对于Active Directory、唯一名称是与关联的名称 `sAMAccountName` 属性。对于OpenLDAP、唯一名称是与关联的名称 `uid` 属性。
3. 选择 * 继续 * 。

管理组权限

组权限控制用户可在租户管理器和租户管理API中执行的任务。

步骤

1. 对于*Access mode*，请选择以下选项之一：
   - 读写(默认)：用户可以登录到租户管理器并管理租户配置。
   - * 只读 * ：用户只能查看设置和功能。他们无法在租户管理器或租户管理API中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。

   > 如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。

2. 如果组用户需要登录到租户管理器或租户管理API、请选中* root访问*复选框。
3. 选择 * 继续 * 。

设置**Swift**组策略

Swift用户需要管理员权限才能通过Swift REST API的身份验证来创建容器和导入对象。

1. 如果组用户需要使用Swift REST API来管理容器和对象、请选中* Swift administrator*复选框。
2. 如果要创建本地组，请选择 * 继续 * 。如果要创建联合组，请选择 * 创建组 * 和 * 完成 * 。

添加用户（仅限本地组）

您可以保存组而不添加用户、也可以选择添加任何已存在的本地用户。

步骤

1. 或者，为此组选择一个或多个本地用户。

   如果尚未创建本地用户、则可以在用户页面上将此组添加到用户。请参见 "管理本地用户"。

2. 选择 * 创建组 * 和 * 完成 * 。

   您创建的组将显示在组列表中。

租户管理权限

在创建租户组之前，请考虑要分配给该组的权限。租户管理权限用于确定用户可以使用租户管理器或租户管理 API 执行的任务。一个用户可以属于一个或多个组。如果用户属于多个组，则权限是累积的。

要登录到租户管理器或使用租户管理 API ，用户必须属于至少具有一个权限的组。所有可以登录的用户均可执行以下任务：

- 查看信息板
- 更改自己的密码（适用于本地用户）

对于所有权限，组的访问模式设置将确定用户是否可以更改设置并执行操作，或者是否只能查看相关设置和功能。

如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。

您可以为组分配以下权限。请注意， S3 租户和 Swift 租户具有不同的组权限。

权限	Description
root 访问权限	提供对租户管理器和租户管理 API 的完全访问权限。 注意： Swift用户必须具有root访问权限才能登录到租户帐户。
管理员	仅限 Swift 租户。提供对此租户帐户的 Swift 容器和对象的完全访问权限 • 注： * Swift 用户必须具有 Swift 管理员权限才能使用 Swift REST API 执行任何操作。
管理您自己的S3凭据	允许用户创建和删除自己的 S3 访问密钥。没有此权限的用户看不到*storage (S3)*>*My S3 access keys*菜单选项。
管理所有存储分段	• S3 租户：允许用户使用租户管理器和租户管理 API 创建和删除 S3 存储分段，并管理租户帐户中所有 S3 存储分段的设置，而不管 S3 存储分段或组策略如何。 没有此权限的用户看不到“存储桶”菜单选项。 • Swift 租户：允许 Swift 用户使用租户管理 API 控制 Swift 容器的一致性级别。 *注意：*您只能从租户管理API为Swift组分配"管理所有存储分段"权限。您不能使用租户管理器将此权限分配给Swift组。
管理端点	允许用户使用租户管理器或租户管理API创建或编辑平台服务端点、这些端点用作StorageGRID 平台服务的目标。 没有此权限的用户看不到“平台服务端点”菜单选项。
使用S3控制台管理对象	与管理所有存储分段权限结合使用时、允许用户从存储分段页面访问体验S3控制台。具有此权限但不具有"管理所有存储分段"权限的用户仍可直接导航到体验S3控制台。

管理组

您可以查看组；编辑组的名称、权限、策略和用户；复制组； 或删除组。

开始之前

- 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"。

查看或编辑组

您可以查看和编辑每个组的基本信息和详细信息。

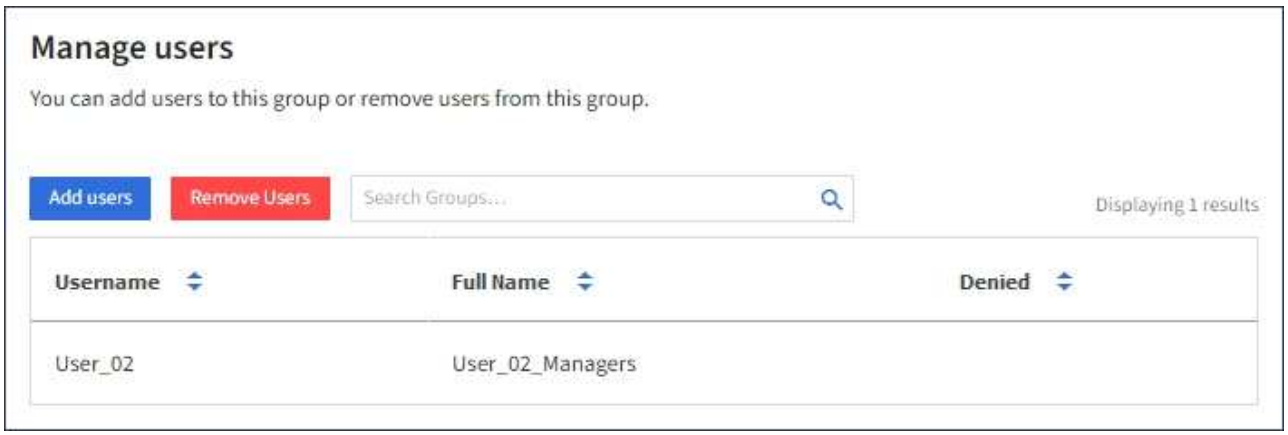
步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 查看"组"页面上提供的信息、其中列出了此租户帐户的所有本地组和联盟组的基本信息。

   如果租户帐户具有*使用网格联合连接*权限、并且您正在查看租户源网格上的组、则蓝色横幅表示、如果您编辑或删除某个组、您所做的更改不会同步到另一个网格。请参见 "克隆租户组和用户"。

3. 如果要更改组的名称：
   a. 选中组对应的复选框。
   b. 选择 * 操作 * > * 编辑组名称 * 。
   c. 输入新名称。
   d. 选择*保存更改。*
4. 如果要查看更多详细信息或进行其他编辑、请执行以下操作之一：
   - 选择组名称。
   - 选中组对应的复选框，然后选择*Actions*>*查看组详细信息*。
5. 查看概述部分、其中显示了每个组的以下信息：
   - 显示名称
   - 唯一名称
   - Type
   - 访问模式
   - 权限
   - S3策略
   - 此组中的用户数
   - 如果租户帐户具有*使用网格联合连接*权限且您正在查看租户源网格上的组、则添加以下字段：
     - 克隆状态：成功*或*失败
     - 蓝色横幅、表示编辑或删除此组时、您所做的更改不会同步到其他网格。
6. 根据需要编辑组设置。请参见 "为 S3 租户创建组" 和 "为 Swift 租户创建组" 有关输入内容的详细信息。
   a. 在概述部分中、通过选择名称或编辑图标来更改显示名称 。
   b. 在*组权限*选项卡上，更新权限，然后选择*保存更改*。
   c. 在*组策略*选项卡上，进行任何更改，然后选择*保存更改*。
      - 如果要编辑S3组、也可以根据需要选择其他S3组策略或输入自定义策略的JSON字符串。
      - 如果要编辑Swift组，可以选择选中或清除*Swift管理员*复选框。

7. 要将一个或多个现有本地用户添加到组、请执行以下操作：
   a. 选择用户选项卡。



   b. 选择*添加用户*。
   c. 选择要添加的现有用户，然后选择*添加用户*。

      右上角将显示一条成功消息。

8. 要从组中删除本地用户、请执行以下操作：
   a. 选择用户选项卡。
   b. 选择*删除用户*。
   c. 选择要去除的用户，然后选择*Remove Users *。

      右上角将显示一条成功消息。

9. 确认您为每个更改的部分选择了*保存更改*。

重复的组

您可以复制现有组、以更快地创建新组。

> 如果您的租户帐户具有*使用网格联合连接*权限、而您从租户的源网格复制了一个组、则复制的组将克隆到租户的目标网格。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选中要复制的组对应的复选框。
3. 选择 * 操作 * > * 复制组 * 。
4. 请参见 "为 S3 租户创建组" 或 "为 Swift 租户创建组" 有关输入内容的详细信息。
5. 选择 * 创建组 * 。

删除一个或多个组

您可以删除一个或多个组。仅属于已删除组的任何用户将无法再登录到租户管理器或使用租户帐户。

如果您的租户帐户具有*使用网格联合连接*权限、而您删除了某个组、则StorageGRID 不会删除另一个网格上的相应组。如果需要保持此信息同步、则必须从两个网格中删除同一个组。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选中要删除的每个组对应的复选框。
3. 选择*Actions*>*Delete group*或*Actions*>*Delete Groups*。

   此时将显示确认对话框。

4. 选择*删除组*或*删除组*。

管理本地用户

您可以创建本地用户并将其分配给本地组，以确定这些用户可以访问哪些功能。租户管理器包括一个预定义的本地用户、名为"`root.`" 虽然您可以添加和删除本地用户、但不能删除root用户。

如果为StorageGRID 系统启用了单点登录(SSO)、则本地用户将无法登录到租户管理器或租户管理API、尽管他们可以根据组权限使用客户端应用程序访问租户的资源。

开始之前

- 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"。
- 如果您的租户帐户具有*使用网格联合连接*权限、则您已查看的工作流和注意事项 "克隆租户组和用户"，您将登录到租户的源网格。

创建本地用户

您可以创建本地用户并将其分配给一个或多个本地组、以控制其访问权限。

不属于任何组的S3用户不具有管理权限或应用了S3组策略。这些用户可能已通过存储分段策略授予 S3 存储分段访问权限。

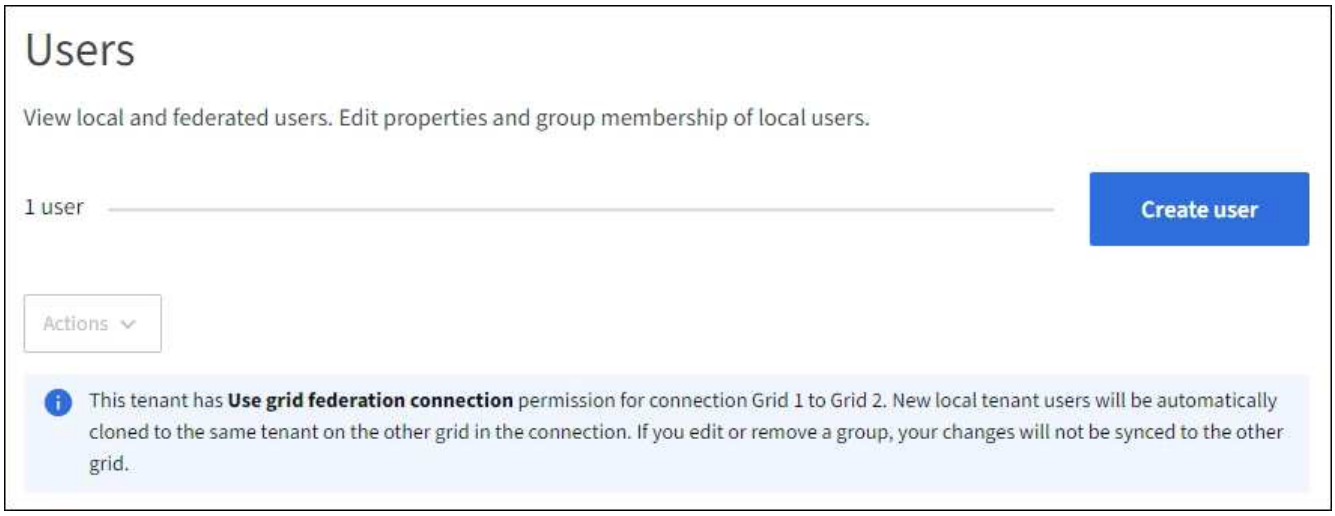
不属于任何组的Swift用户没有管理权限或Swift容器访问权限。

访问创建用户向导

步骤

1. 选择 * 访问管理 * > * 用户 * 。

   如果您的租户帐户具有*使用网格联合连接*权限、则蓝色横幅指示这是租户的源网格。您在此网格上创建的任何本地用户都将克隆到连接中的另一个网格。



2. 选择 * 创建用户 * 。

输入凭据

步骤

1. 对于*输入用户凭据*步骤，请填写以下字段。

字段	Description
全名	此用户的全名、例如、人员的名字和姓氏或应用程序的名称。
Username	此用户用于登录的名称。用户名必须唯一、并且无法更改。 注意：如果您的租户帐户具有*使用网格联合连接*权限、则如果目标网格上的租户已存在相同的*用户名*、则会发生克隆错误。
密码和确认密码	用户在登录时最初使用的密码。
拒绝访问	选择*是*可防止此用户登录到租户帐户、即使他们可能仍属于一个或多个组也是如此。 例如，选择*Yes*可暂时暂停用户的登录能力。

2. 选择 * 继续 * 。

分配给组

步骤

1. 将用户分配给一个或多个本地组、以确定他们可以执行哪些任务。

   将用户分配到组是可选的。如果您愿意、可以在创建或编辑组时选择用户。

   不属于任何组的用户将无管理权限。权限是累积的。用户将对其所属的所有组拥有所有权限。请参见 "租户管理权限"。

2. 选择 * 创建用户 * 。

   如果您的租户帐户具有*使用网格联合连接*权限、而您位于租户的源网格上、则新的本地用户将克隆到租户的目标网格。在用户的详细信息页面的"概述"部分中、成功*显示为*克隆状态。

3. 选择*完成*返回用户页。

查看或编辑本地用户

步骤

1. 选择 * 访问管理 * > * 用户 * 。
2. 查看"用户"页面上提供的信息、其中列出了此租户帐户的所有本地和联盟用户的基本信息。

   如果租户帐户具有*使用网格联合连接*权限、而您正在租户的源网格上查看用户、则蓝色横幅指示编辑或删除用户时、您所做的更改不会同步到其他网格。

3. 如果要更改用户的全名：
   a. 选中用户对应的复选框。
   b. 选择 * 操作 * > * 编辑全名 * 。
   c. 输入新名称。
   d. 选择*保存更改。*
4. 如果要查看更多详细信息或进行其他编辑、请执行以下操作之一：
   - 选择用户名。
   - 选中用户对应的复选框，然后选择*Actions*>*查看用户详细信息*。
5. 查看概述部分、其中显示了每个用户的以下信息：
   - 全名
   - Username
   - 用户类型
   - 拒绝访问
   - 访问模式
   - 组成员资格
   - 如果租户帐户具有*使用网格联合连接*权限且您正在查看租户源网格上的用户、则添加以下字段：
     - 克隆状态：成功*或*失败
     - 蓝色横幅、表示如果编辑此用户、您所做的更改不会同步到其他网格。
6. 根据需要编辑用户设置。请参见 创建本地用户 有关输入内容的详细信息。
   a. 在概述部分中、选择名称或编辑图标以更改全名  。

      您不能更改用户名。

   b. 在*密码*选项卡上，更改用户的密码，然后选择*保存更改*。
   c. 在*访问*选项卡上，选择*否*允许用户登录，或选择*是*阻止用户登录。然后，选择*保存更改*。

d. 在*Access keys*选项卡上，选择*Create key*并按照的说明进行操作 "正在创建其他用户的S3访问密钥"。

e. 在*组*选项卡上，选择*编辑组*将用户添加到组或从组中删除用户。然后，选择*保存更改*。

7. 确认您为每个更改的部分选择了*保存更改*。

本地用户重复

您可以复制本地用户以更快地创建新用户。

> 如果您的租户帐户具有*使用网格联合连接*权限、而您从租户的源网格复制了一个用户、则复制的用户将克隆到租户的目标网格。

步骤

1. 选择 * 访问管理 * > * 用户 * 。
2. 选中要复制的用户对应的复选框。
3. 选择 * 操作 * > * 复制用户 * 。
4. 请参见 创建本地用户 有关输入内容的详细信息。
5. 选择 * 创建用户 * 。

删除一个或多个本地用户

您可以永久删除一个或多个不再需要访问StorageGRID 租户帐户的本地用户。

> 如果您的租户帐户具有*使用网格联合连接*权限、而您删除了本地用户、则StorageGRID 不会删除其他网格上的相应用户。如果需要使此信息保持同步、则必须从两个网格中删除同一用户。

> 您必须使用联合身份源删除联合用户。

步骤

1. 选择 * 访问管理 * > * 用户 * 。
2. 选中要删除的每个用户对应的复选框。
3. 选择*Actions*>*Delete user*或*Actions*>*Delete user*。

   此时将显示确认对话框。

4. 选择*删除用户*或*删除用户*。

管理 S3 访问密钥

管理S3访问密钥：概述

S3 租户帐户的每个用户都必须具有访问密钥，才能在 StorageGRID 系统中存储和检索对象。访问密钥由访问密钥 ID 和机密访问密钥组成。

S3 访问密钥可按如下方式进行管理：

- 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访问权限*的用户可以管理S3 root帐户和所有其他用户的访问密钥。除非存储分段策略明确禁用，否则根访问密钥可为租户提供对所有存储分段和对象的完全访问权限。

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

创建您自己的 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以创建自己的 S3 访问密钥。您必须具有访问密钥才能访问分段和对象。

开始之前

- 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 "管理您自己的S3凭据或root访问权限"。

关于此任务

您可以创建一个或多个 S3 访问密钥，以便为租户帐户创建和管理存储分段。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。为了安全起见、请勿创建超出所需数量的密钥、并删除未使用的密钥。如果只有一个密钥，并且该密钥即将到期，请在旧密钥到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，也可以无到期时间。请遵循以下到期时间准则：

- 为密钥设置到期时间，以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访问密钥 ID 和机密访问密钥意外暴露时的风险。过期密钥将自动删除。
- 如果环境中的安全风险较低、并且您不需要定期创建新密钥、则不必设置密钥的到期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。

> 您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用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，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。

   此时将显示 My access keys 页面，其中列出了所有现有访问密钥。

2. 选择 * 创建密钥 * 。
3. 执行以下操作之一：
   - 选择 * 不设置到期时间 * 可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。

     > 到期日期最多可以是自当前日期起五年。到期时间至少可以是当前时间之后的一分钟。

4. 选择 * 创建访问密钥 * 。

此时将显示 Download access key 对话框，其中列出了您的访问密钥 ID 和机密访问密钥。

5. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

   复制或下载此信息之前、请勿关闭此对话框。关闭对话框后、您无法复制或下载密钥。

6. 选择 * 完成 * 。

   新密钥将列在 " 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、也可以使用租户管理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。请参见 "使用API克隆S3访问密钥"。

查看 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以查看 S3 访问密钥列表。您可以按到期时间对列表进行排序，以便确定哪些密钥不久将过期。您可以根据需要执行此操作 "创建新密钥" 或 "删除密钥" 您不再使用的。

您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用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，并且切勿与其他用户共享这些密钥。

开始之前

- 您将使用登录到租户管理器 "支持的 Web 浏览器"。
- 您所属的用户组具有管理您自己的S3凭据 "permission"。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。
2. 在“我的访问密钥”页面中，按*Expiration time*或*Access key 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任何密钥。

   如果在现有密钥到期之前创建新密钥，则可以开始使用新密钥，而不会暂时丢失对帐户中对象的访问权限。

   过期密钥将自动删除。

删除您自己的 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以删除您自己的 S3 访问密钥。删除访问密钥后，无法再使用它访问租户帐户中的对象和分段。

开始之前

- 您将使用登录到租户管理器 "支持的 Web 浏览器"。
- 您具有管理自己的 S3 凭据权限。请参见 "租户管理权限"。

您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用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，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。
2. 在我的访问密钥页面中、选中要删除的每个访问密钥对应的复选框。
3. 选择 * 删除密钥 * 。
4. 从确认对话框中，选择*Delete key*。

   页面右上角将显示一条确认消息。

创建其他用户的 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以为其他用户创建 S3 访问密钥，例如需要访问存储分段和对象的应用程序。

开始之前

- 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"。

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，以便他们可以为其租户帐户创建和管理存储分段。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。为了安全起见、请不要创建超出用户需要的密钥、并删除未使用的密钥。如果只有一个密钥，并且该密钥即将到期，请在旧密钥到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，也可以无到期时间。请遵循以下到期时间准则：

- 设置密钥的到期时间，以将用户的访问限制为特定时间段。如果访问密钥 ID 和机密访问密钥意外暴露，则设置较短的到期时间有助于降低风险。过期密钥将自动删除。
- 如果环境中的安全风险较低、并且您不需要定期创建新密钥、则不必设置密钥的到期时间。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用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

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 * 访问密钥 * ，然后选择 * 创建密钥 * 。

4. 执行以下操作之一：
   - 选择*不设置到期时间*以创建不到期的密钥。（默认）
   - 选择 * 设置到期时间 * ，然后设置到期日期和时间。

     到期日期最多可以是自当前日期起五年。到期时间至少可以是当前时间之后的一分钟。

5. 选择 * 创建访问密钥 * 。

   此时将显示 Download access key 对话框，其中列出了访问密钥 ID 和机密访问密钥。

6. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

   复制或下载此信息之前、请勿关闭此对话框。关闭对话框后、您无法复制或下载密钥。

7. 选择 * 完成 * 。

   新密钥将列在用户详细信息页面的访问密钥选项卡中。

8. 如果您的租户帐户具有*使用网格联合连接*权限、也可以使用租户管理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。请参见 "使用API克隆S3访问密钥"。

查看其他用户的 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，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，以便确定哪些密钥不久将过期。您可以根据需要创建新密钥并删除不再使用的密钥。

开始之前

- 您将使用登录到租户管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

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. 从“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。

   如果在现有密钥到期之前创建新密钥，则用户可以开始使用新密钥，而不会暂时丢失对帐户中对象的访问权限。

过期密钥将自动删除。

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"

删除其他用户的 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以删除其他用户的 S3 访问密钥。删除访问密钥后，无法再使用它访问租户帐户中的对象和分段。

开始之前

- 您将使用登录到租户管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。请参见 "租户管理权限"。

> 可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

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*访问密钥*，然后选中要删除的每个访问密钥对应的复选框。
4. 选择 * 操作 * > * 删除选定密钥 * 。
5. 从确认对话框中，选择*Delete key*。

   页面右上角将显示一条确认消息。

管理 S3 存储分段

创建 S3 存储区。

您可以使用租户管理器为对象数据创建 S3 分段。

开始之前

- 您将使用登录到租户管理器 "支持的 Web 浏览器"。
- 您属于具有root访问权限或管理所有分段的用户组 "permission"。这些权限将覆盖组或存储分段策略中的权限设置。

  > 可以授予设置或修改存储分段或对象的 S3 对象锁定属性的权限 "存储分段策略或组策略"。

- 如果您计划为存储分段启用S3对象锁定、则网格管理员已为StorageGRID 系统启用全局S3对象锁定设置、并且您已查看S3对象锁定分段和对象的要求。请参见 "使用S3对象锁定保留对象"。

访问向导

步骤

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

输入详细信息

步骤

1. 输入存储分段的详细信息。

字段	Description
Bucket Name	符合以下规则的存储分段名称： • 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。 • 必须符合 DNS 要求。 • 必须至少包含 3 个字符，并且不能超过 63 个字符。 • 每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。 • 不应在虚拟托管模式请求中使用句点。句点会在验证服务器通配符证书时出现发生原因 问题。 有关详细信息，请参见 "有关存储分段命名规则的 Amazon Web Services （ AWS ）文档"。 注意:创建存储分段后不能更改存储分段名称。
Region	存储分段的区域。 StorageGRID 管理员负责管理可用的区域。存储分段的区域可能会影响应用于对象的数据保护策略。默认情况下、所有分段都在中创建 `us-east-1` 区域。 注意：创建存储分段后无法更改区域。

2. 选择 * 继续 * 。

管理对象设置

步骤

1. （可选）为存储分段启用对象版本控制。

   如果要将每个对象的每个版本存储在此存储分段中，请启用对象版本控制。然后，您可以根据需要检索对象的先前版本。如果要使用分段进行跨网格复制、则必须启用对象版本控制。

2. 如果启用了全局S3对象锁定设置、则可以选择为存储分段启用S3对象锁定、以便使用一次写入、多次读取(WORM)模型存储对象。

只有在需要将对象保留固定时间(例如为了满足特定法规要求)时、才为存储分段启用S3对象锁定。S3对象锁定是一种永久设置、可帮助您防止在固定时间内或无限期删除或覆盖对象。

> 为存储分段启用S3对象锁定设置后、便无法将其禁用。具有正确权限的任何人都可以向此存储分段添加无法更改的对象。您可能无法删除这些对象或存储分段本身。

如果为存储分段启用 S3 对象锁定，则会自动启用存储分段版本控制。

3. 如果选择了*启用S3对象锁定*，则可以选择为此存储分段启用*默认保留*。

   启用*默认保留*后，添加到存储分段的新对象将自动受到保护，不会被删除或覆盖。*默认保留*设置不适用于具有自己保留期限的对象。

   a. 如果启用了*默认保留*，请为存储分段指定*默认保留模式*。

默认保留模式	Description
合规性	• 在达到保留截止日期之前、无法删除此对象。 • 对象的保留截止日期可以增加、但不能减少。 • 在达到该日期之前、无法删除对象的保留截止日期。
监管	• 使用的用户 `s3:BypassGovernanceRetention` 权限可以使用 `x-amz-bypass-governance-retention: true` 请求标头以绕过保留设置。 • 这些用户可以在达到保留截止日期之前删除对象版本。 • 这些用户可以增加、减少或删除对象的保留截止日期。

   b. 如果启用了*默认保留*，请指定存储分段的*默认保留期限*。

      *默认保留期限*表示添加到此存储分段的新对象应保留多长时间、从其被插入开始。指定一个介于1到36、500天之间或介于1到100年之间(含1到100年)的值。

4. 选择 * 创建存储分段 * 。

   此时将创建存储分段并将其添加到 " 存储分段 " 页面上的表中。

5. (可选)选择*转至存储分段详细信息页面*至 "查看存储分段详细信息" 并执行其他配置。

查看存储分段详细信息

您可以查看租户帐户中的存储分段。

开始之前

- 您将使用登录到租户管理器 "支持的 Web 浏览器"。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。

此时将显示"分段"页面。

2. 查看每个存储分段的摘要信息。

   您可以根据需要按任何列对信息进行排序，也可以在列表中向前和向后翻页。

   显示的对象计数和已用空间值为估计值。这些估计值受载入时间，网络连接和节点状态的影响。如果分段启用了版本控制，则删除的对象版本将包含在对象计数中。

列	Description
Name	存储分段的唯一名称、无法更改。
已启用的功能	为存储分段启用的功能列表。
S3 对象锁定	是否为存储分段启用S3对象锁定。 只有在为网格启用了S3对象锁定时、才会显示此列。此列还会显示任何旧版合规存储分段的信息。
Region	无法更改的存储分段区域。
对象计数	此分段中的对象数。添加或删除对象时、此值可能不会立即更新。如果分段启用了版本控制、则此值将包含非当前对象版本。
已用空间	分段中所有对象的逻辑大小。逻辑大小不包括复制的或经过纠删编码的副本或对象元数据所需的实际空间。
创建日期	创建存储分段的日期和时间。

3. 要查看特定存储分段的详细信息、请从表中选择存储分段名称。

   此时将显示存储分段详细信息页面。在此页面中、您可以执行以下任务：

   - 配置和管理存储分段选项、例如 "一致性级别"， "上次访问时间更新"， "对象版本控制"， "S3 对象锁定" 和 "默认存储分段保留"
   - 配置存储分段访问、例如 "跨源资源共享(CORS)"
   - 管理 "平台服务" (如果允许租户使用)、包括复制、事件通知和搜索集成
   - 启用和 "管理跨网格复制" (如果租户允许)将此存储分段中的对象复制到另一个StorageGRID 系统
   - 访问 "试验性S3控制台" 以管理存储分段中的对象
   - "删除存储分段中的所有对象"
   - "删除存储分段" 该值已为空

更改存储分段的一致性级别

如果您使用的是S3租户、则可以更改对S3存储分段中的对象执行操作的一致性级别。

开始之前

- 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 "管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。

关于此任务

一致性控制可以在对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。通常，您应该对存储分段使用 * 读 - 后 - 新 - 写 * 一致性级别。

如果*读后新写入*一致性级别不符合客户端应用程序的要求、则可以通过设置存储分段一致性级别或使用来更改一致性级别 `Consistency-Control` 标题。。 `Consistency-Control` 标题将覆盖存储分段一致性级别。

> 更改存储分段的一致性级别时，只会保证更改后载入的对象符合修订后的级别。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

3. 从*存储分段选项*选项卡中，选择*一致性级别*可调项。
4. 为此存储分段中的对象选择一个一致性级别。
   - 全部：提供最高级别的一致性。所有节点都会立即接收数据，否则请求将失败。
   - 强-全局：保证所有站点中所有客户端请求的写入后读一致性。
   - 强站点：保证站点内所有客户端请求的写入后读一致性。
   - 读后新写入(默认)：为新对象提供读后写入一致性、并最终为对象更新提供一致性。提供高可用性和数据保护保证。建议用于大多数情况。
   - 可用：为新对象和对象更新提供最终一致性。对于S3存储分段、请仅在需要时使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行HEAD或GET操作)。S3 FabricPool 存储分段不支持。
5. 选择 * 保存更改 * 。

启用或禁用上次访问时间更新

当网格管理员为 StorageGRID 系统创建信息生命周期管理（ ILM ）规则时，他们可以选择指定对象的最后访问时间来确定是否将该对象移动到其他存储位置。如果您使用的是 S3 租户，则可以通过为 S3 存储分段中的对象启用上次访问时间更新来利用此类规则。

这些说明仅适用于至少包含一个使用*上次访问时间*选项作为高级筛选器或参考时间的ILM规则的StorageGRID系统。如果您的 StorageGRID 系统不包含此类规则，则可以忽略这些说明。请参见 "在ILM规则中使用上次访问时间" 了解详细信息。

开始之前

- 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 "管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。

关于此任务

*上次访问时间*是ILM规则的*参考时间*放置指令的可用选项之一。通过将规则的"参考时间"设置为上次访问时间、网格管理员可以根据上次检索(读取或查看)对象的时间指定将对象放置在某些存储位置。

例如，为了确保最近查看的对象保持在较快的存储上，网格管理员可以创建一个 ILM 规则，指定以下内容：

- 过去一个月检索到的对象应保留在本地存储节点上。
- 过去一个月未检索到的对象应移至异地位置。

默认情况下，对上次访问时间的更新处于禁用状态。如果您的StorageGRID 系统包含使用*上次访问时间*选项的ILM规则、而您希望此选项应用于此存储分段中的对象、则必须为该规则中指定的S3存储分段启用上次访问时间更新。

> 在检索对象时更新上次访问时间会降低 StorageGRID 性能，尤其是对于小型对象。

上次访问时间更新会影响性能，因为每次检索对象时， StorageGRID 都必须执行以下附加步骤：

- 使用新的时间戳更新对象
- 将对象添加到 ILM 队列，以便根据当前 ILM 规则和策略对其进行重新评估

下表汇总了禁用或启用上次访问时间时应用于存储分段中所有对象的行为。

请求类型	禁用上次访问时间时的行为（默认）		启用上次访问时间时的行为	
	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?
请求检索对象，其访问控制列表或其元数据	否	否	是的。	是的。
请求更新对象的元数据	是的。	是的。	是的。	是的。
请求将对象从一个存储分段复制到另一个存储分段	• 否，对于源副本 • 是，对于目标副本	• 否，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本
请求完成多部分上传	是，对于已组装的对象	是，对于已组装的对象	是，对于已组装的对象	是，对于已组装的对象

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

3. 从*存储分段选项*选项卡中，选择*上次访问时间更新*可接触框。
4. 启用或禁用上次访问时间更新。
5. 选择 * 保存更改 * 。

更改存储分段的对象版本控制

如果您使用的是S3租户、则可以更改S3存储分段的版本控制状态。

开始之前

- 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 "管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。

关于此任务

您可以为存储分段启用或暂停对象版本控制。为存储分段启用版本控制后、存储分段无法恢复为未受版本控制的状态。但是，您可以暂停存储分段的版本控制。

- Disabled ： 从未启用版本控制
- Enabled ： 已启用版本控制
- suspended ： 先前已启用版本控制并已暂停

有关详细信息，请参见以下内容：

- "对象版本控制"
- "S3 版本对象的 ILM 规则和策略（示例 4 ）"
- "如何删除对象"

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

3. 从“存储分段选项”选项卡中，选择“对象版本控制”可选框。
4. 为此存储分段中的对象选择版本控制状态。

   对于用于跨网格复制的存储分段、必须始终启用对象版本控制。如果启用了 S3 对象锁定或原有合规性，则会禁用 * 对象版本控制 * 选项。

选项	Description
启用版本控制	如果要将每个对象的每个版本存储在此存储分段中，请启用对象版本控制。然后，您可以根据需要检索对象的先前版本。 用户修改存储分段中已存在的对象时，这些对象将进行版本控制。
暂停版本控制	如果您不再需要创建新的对象版本，请暂停对象版本控制。您仍然可以检索任何现有对象版本。

5. 选择 * 保存更改 * 。

使用S3对象锁定保留对象

如果存储分段和对象必须符合保留法规要求、则可以使用S3对象锁定。

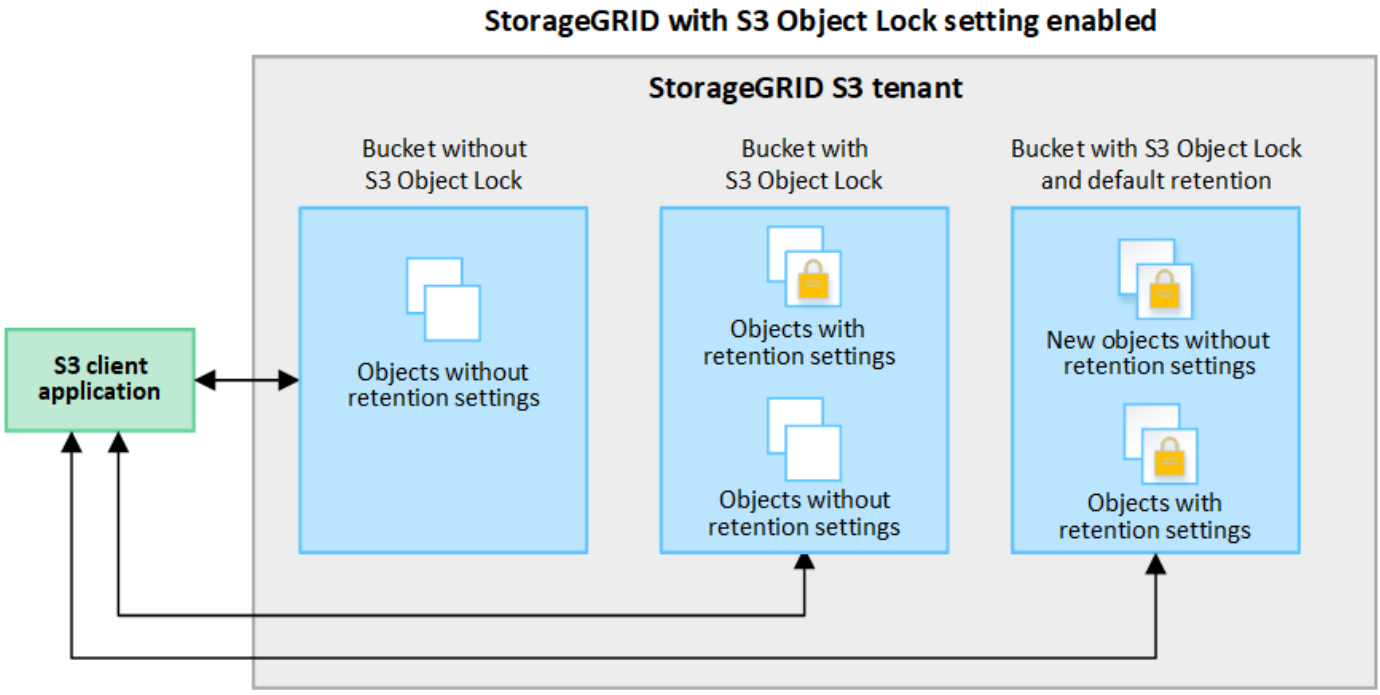
什么是 **S3** 对象锁定?

StorageGRID S3 对象锁定功能是一种对象保护解决方案，相当于 Amazon Simple Storage Service （Amazon S3 ）中的 S3 对象锁定。

如图所示，如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则 S3 租户帐户可以在启用或不启用 S3 对象锁定的情况下创建存储分段。如果存储分段启用了S3对象锁定、则需要执行存储分段版本控制、并会自动启用此功能。

如果存储分段启用了S3对象锁定、S3客户端应用程序可以选择为保存到该存储分段的任何对象版本指定保留设置。

此外、启用了S3对象锁定的分段还可以选择具有默认保留模式和保留期限。默认设置仅适用于添加到存储分段的对象、这些对象没有自己的保留设置。



保留模式

StorageGRID S3对象锁定功能支持两种保留模式、可对对象应用不同级别的保护。这些模式相当于Amazon S3保留模式。

- 在合规模式下：
  - 在达到保留截止日期之前、无法删除此对象。
  - 对象的保留截止日期可以增加、但不能减少。
  - 在达到该日期之前、无法删除对象的保留截止日期。
- 在监管模式下：
  - 具有特殊权限的用户可以在请求中使用旁路标头来修改某些保留设置。
  - 这些用户可以在达到保留截止日期之前删除对象版本。
  - 这些用户可以增加、减少或删除对象的保留截止日期。

对象版本的保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以使用S3客户端应用程序为添加到该存储分段的每个对象指定以下保留设置(可选)：

- 保留模式：合规性或监管。
- **retain**至日期：如果某个对象版本的retain至日期为未来版本，则可以检索该对象，但不能将其删除。
- * 合法保留 * ：对对象版本应用合法保留时，会立即锁定该对象。例如，您可能需要对与调查或法律争议相关的对象进行法律保留。合法保留没有到期日期，但在明确删除之前始终有效。合法保留与保留日期无关。

> 如果某个对象处于合法保留状态、则无论其保留模式如何、任何人都无法删除该对象。

有关对象设置的详细信息、请参见 "使用S3 REST API配置S3对象锁定"。

存储分段的默认保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以选择为此存储分段指定以下默认设置：

- 默认保留模式：合规或监管。
- 默认保留期限：添加到此存储分段的新对象版本应保留多长时间、从添加之日开始。

默认分段设置仅适用于没有自己的保留设置的新对象。添加或更改这些默认设置时、现有存储分段对象不会受到影响。

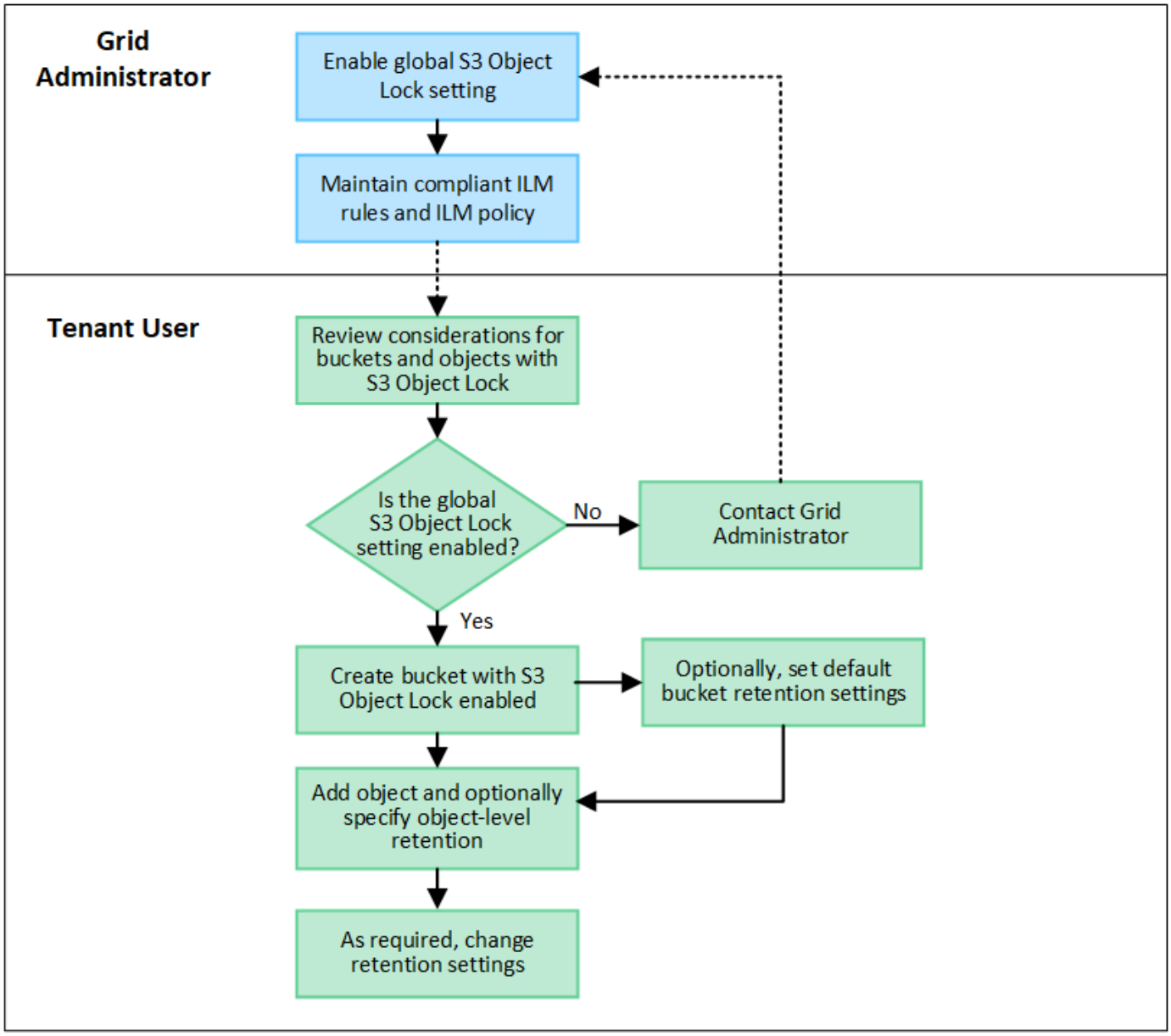
请参见 "创建 S3 存储区。" 和 "更新S3对象锁定默认保留"。

S3 对象锁定工作流

工作流图显示了在 StorageGRID 中使用 S3 对象锁定功能的高级步骤。

在启用了 S3 对象锁定的情况下创建分段之前，网格管理员必须为整个 StorageGRID 系统启用全局 S3 对象锁定设置。网格管理员还必须确保信息生命周期管理(ILM)策略"`compliant`"；它必须满足启用了S3对象锁定的分段的要求。有关详细信息、请与网格管理员联系或参见的说明 "使用S3对象锁定管理对象"。

启用全局S3对象锁定设置后、您可以在启用S3对象锁定的情况下创建存储分段、也可以为每个存储分段指定默认保留设置。此外、您还可以使用S3客户端应用程序为每个对象版本指定保留设置(可选)。



启用了 **S3** 对象锁定的存储分段的要求

- 如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以使用租户管理器，租户管理 API 或 S3 REST API 创建启用了 S3 对象锁定的分段。
- 如果您计划使用 S3 对象锁定，则必须在创建存储分段时启用 S3 对象锁定。您不能为现有存储分段启用S3对象锁定。
- 为存储分段启用 S3 对象锁定后， StorageGRID 会自动为该存储分段启用版本控制。您不能禁用存储分段的S3对象锁定或暂停版本控制。
- 您也可以使用租户管理器、租户管理API或S3 REST API为每个存储分段指定默认保留模式和保留期限。存储分段的默认保留设置仅适用于添加到存储分段中但没有自己的保留设置的新对象。您可以通过在上传每个对象版本时为其指定保留模式和保留截止日期来覆盖这些默认设置。
- 启用了S3对象锁定的分段支持分段生命周期配置。

- 启用了 S3 对象锁定的存储分段不支持 CloudMirror 复制。

启用了 **S3** 对象锁定的分段中的对象的要求

- 要保护对象版本、您可以为存储分段指定默认保留设置、也可以为每个对象版本指定保留设置。可以使用S3客户端应用程序或S3 REST API指定对象级保留设置。
- 保留设置适用于各个对象版本。对象版本可以同时具有保留截止日期和合法保留设置，但不能具有其他设置，或者两者均不具有。为对象指定保留日期或合法保留设置仅保护请求中指定的版本。您可以创建新版本的对象，而先前版本的对象仍保持锁定状态。

启用了 **S3** 对象锁定的存储分段中的对象生命周期

在启用了S3对象锁定的情况下保存在存储分段中的每个对象都会经历以下阶段：

1. * 对象载入 *

   将对象版本添加到启用了S3对象锁定的存储分段时、将按如下所示应用保留设置：

   - 如果为对象指定了保留设置、则会应用对象级别设置。系统将忽略任何默认存储分段设置。
   - 如果没有为对象指定保留设置、则会应用默认存储分段设置(如果存在)。
   - 如果没有为对象或存储分段指定保留设置、则对象不受S3对象锁定保护。

   如果应用了保留设置、则对象和任何S3用户定义的元数据都会受到保护。

2. 对象保留和删除

   StorageGRID 会在指定的保留期限内存储每个受保护对象的多个副本。对象副本的确切数量和类型以及存储位置由活动ILM策略中的合规规则决定。是否可以在达到保留截止日期之前删除受保护对象取决于其保留模式。

   - 如果某个对象处于合法保留状态、则无论其保留模式如何、任何人都无法删除该对象。

是否仍可管理旧版合规存储分段?

S3 对象锁定功能取代了先前 StorageGRID 版本中提供的合规性功能。如果您使用早期版本的 StorageGRID 创建了合规的存储分段，则可以继续管理这些存储分段的设置；但是，您无法再创建新的合规存储分段。有关说明，请参见https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"^]。

更新**S3**对象锁定默认保留

如果您在创建存储分段时启用了S3对象锁定、则可以编辑存储分段以更改默认保留设置。您可以启用(或禁用)默认保留并设置默认保留模式和保留期限。

开始之前

- 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 "管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。

- 系统会为您的StorageGRID 系统全局启用S3对象锁定、您可以在创建存储分段时启用S3对象锁定。请参见 "使用S3对象锁定保留对象"。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

3. 从*存储分段选项*选项卡中，选择*S3对象锁定*可触摸板。
4. (可选)为此存储分段启用或禁用*默认保留*。

   对此设置所做的更改不会应用于存储分段中已有的对象或可能具有自己保留期限的任何对象。

5. 如果启用了*默认保留*，请为存储分段指定*默认保留模式*。

默认保留模式	Description
合规性	• 在达到保留截止日期之前、无法删除此对象。 • 对象的保留截止日期可以增加、但不能减少。 • 在达到该日期之前、无法删除对象的保留截止日期。
监管	• 使用的用户 `s3:BypassGovernanceRetention` 权限可以使用 `x-amz-bypass-governance-retention: true` 请求标头以绕过保留设置。 • 这些用户可以在达到保留截止日期之前删除对象版本。 • 这些用户可以增加、减少或删除对象的保留截止日期。

6. 如果启用了*默认保留*，请指定存储分段的*默认保留期限*。

   *默认保留期限*表示添加到此存储分段的新对象应保留多长时间、从其被插入开始。指定一个介于1到36、500天之间或介于1到100年之间(含1到100年)的值。

7. 选择 * 保存更改 * 。

配置跨源资源共享（ CORS ）

如果您希望S3存储分段和该存储分段中的对象可供其他域中的Web应用程序访问、则可以为该存储分段配置跨源站资源共享(CORS)。

开始之前

- 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 "管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。

关于此任务

跨源资源共享（ CORS ）是一种安全机制，允许一个域中的客户端 Web 应用程序访问不同域中的资源。例如、

假设您使用名为的S3存储分段 `Images` 以存储图形。通过为配置CORS `Images` 存储分段中的图像、您可以在网站上显示该存储分段中的图像 `http://www.example.com`。

为存储分段启用**CORS**

步骤

1. 使用文本编辑器创建所需的XML。

   此示例显示了用于为 S3 存储分段启用 CORS 的 XML 。此XML允许任何域向存储分段发送GET请求、但仅允许 `http://www.example.com` 用于发送POST和删除请求的域。允许使用所有请求标头。

   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedMethod>POST</AllowedMethod>
           <AllowedMethod>DELETE</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
   </CORSConfiguration>
   ```

   有关 CORS 配置 XML 的详细信息，请参见 "Amazon Web Services （ AWS ）文档：《 Amazon Simple Storage Service 开发人员指南》"。

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. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

4. 从*存储分段访问*选项卡中，选择*跨源资源共享(CORS)*可接触式。
5. 选中*启用CORS*复选框。
6. 将CORS配置XML粘贴到文本框中。
7. 选择 * 保存更改 * 。

修改**CORS**设置

步骤

1. 更新文本框中的CORS配置XML，或选择*Clear*重新开始。
2. 选择 * 保存更改 * 。

禁用**CORS**设置

步骤

1. 清除*启用CORS*复选框。
2. 选择 * 保存更改 * 。

删除存储分段中的对象

您可以使用租户管理器删除一个或多个存储分段中的对象。

注意事项和要求

在执行这些步骤之前、请注意以下事项：

- 删除存储分段中的对象后、StorageGRID 会从StorageGRID 系统中的所有节点和站点中永久删除每个选定存储分段中的所有对象和所有对象版本。StorageGRID 还会删除任何相关的对象元数据。您将无法恢复此信息。
- 根据对象数、对象副本数和并发操作数、删除存储分段中的所有对象可能需要几分钟、几天甚至几周时间。
- 如果存储分段具有 "已启用S3对象锁定"，则它可能会在_yrees_状态下保持*Deleting objects: read-only。

> 使用S3对象锁定的存储分段将保持*删除对象：只读*状态、直到达到所有对象的保留日期并删除任何合法保留为止。

- 删除对象时，存储分段的状态为*删除对象：只读*。在这种状态下、您不能向存储分段添加新对象。
- 删除所有对象后、存储分段将保持只读状态。您可以执行以下操作之一：
  - 将存储分段恢复为写入模式、并将其用于新对象
  - 删除存储分段
  - 保持存储分段处于只读模式、以保留其名称供将来使用
- 如果存储分段启用了对象版本控制、则在开始这些步骤时、删除对象操作不会删除存储分段中的任何删除标记。如果要在删除所有对象后删除分版本存储分段、则必须删除任何已存在的删除标记。
- 如果您使用 "跨网格复制"，请注意以下事项：
  - 使用此选项不会从其他网格的存储分段中删除任何对象。
  - 如果为源分段选择此选项，则在将对象添加到另一网格上的目标分段时，将触发*跨网格复制失败*警报。如果您无法保证没有人会将对象添加到另一网格的存储分段中、 "禁用跨网格复制" 删除所有存储分段对象之前。

开始之前

- 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"。此权限将覆盖组或存储分段策略中的权限设置。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。

   此时将显示 " 分段 " 页面，其中会显示所有现有的 S3 分段。

2. 使用*操作*菜单或特定存储分段的详细信息页面。

操作菜单

a. 选中要从中删除对象的每个存储分段对应的复选框。

b. 选择*操作*>*删除存储分段中的对象*。

详细信息页面

a. 选择存储分段名称以显示其详细信息。

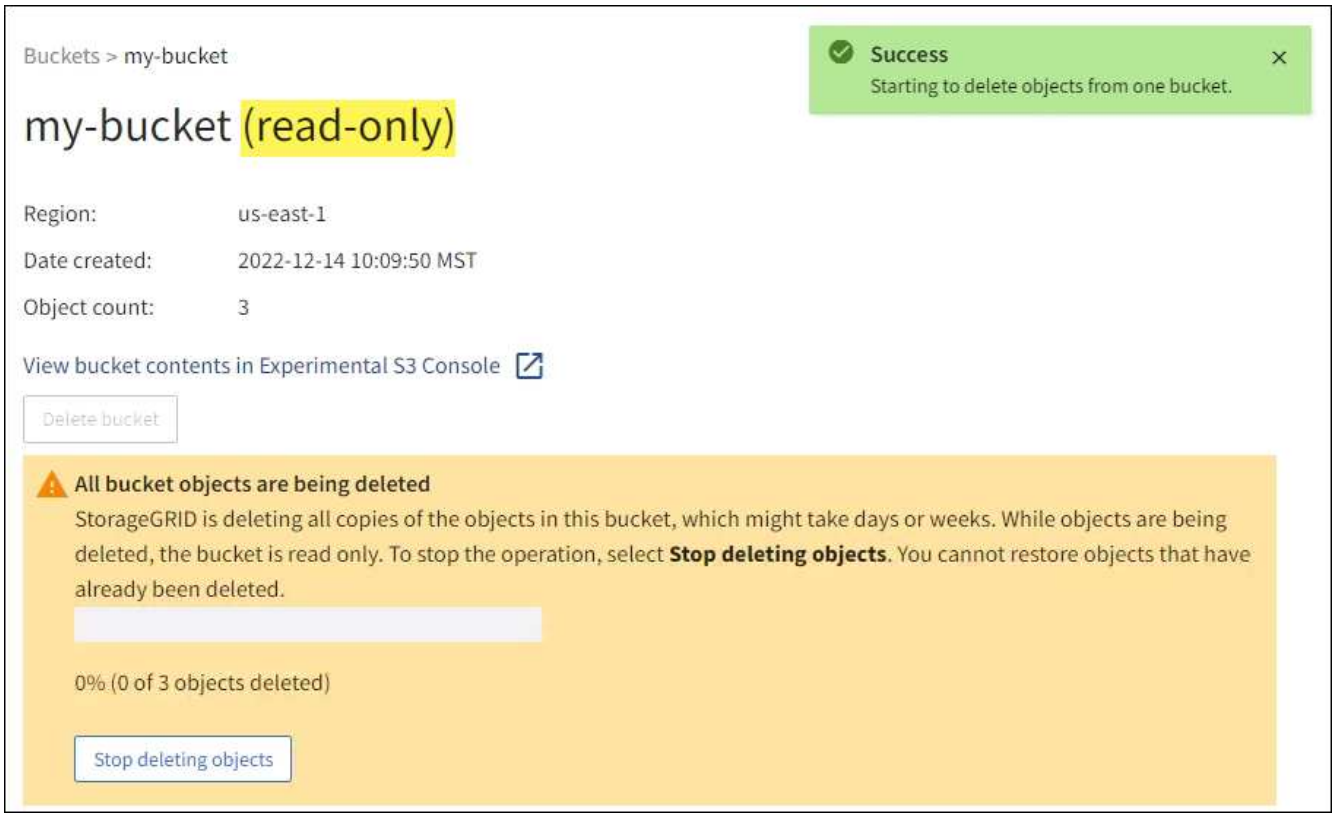
b. 选择*删除存储分段中的对象*。

3. 出现确认对话框时，查看详细信息，输入*Yes*，然后选择*OK*。

4. 等待删除操作开始。

几分钟后：

- 此时、存储分段详细信息页面上将显示一个黄色状态横幅。进度条表示已删除的对象百分比。
- 在存储分段详细信息页面上、*(只读)*显示在存储分段名称后面。
- *(删除对象：只读)*出现在"分段"页的分段名称旁边。

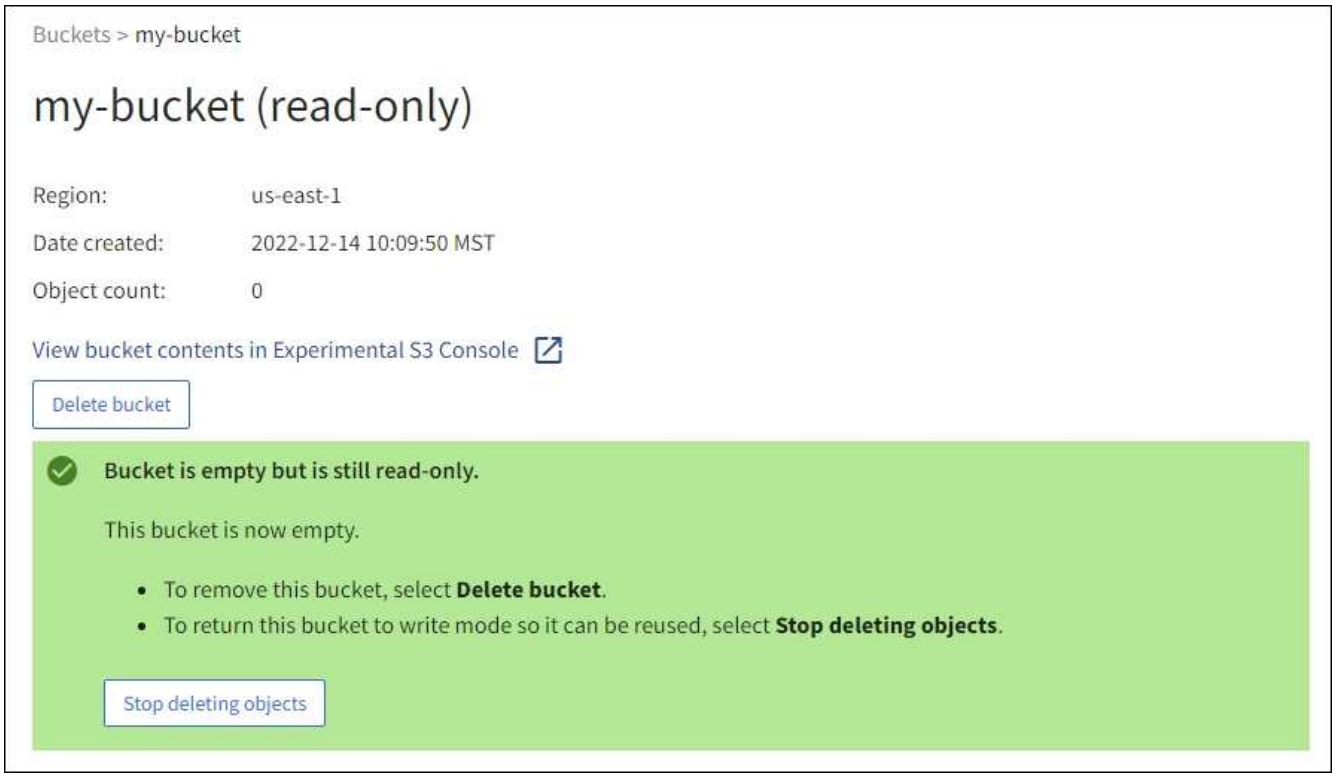


5. 在运行操作时，根据需要选择*停止删除对象*以暂停进程。然后，选择*删除存储分段中的对象*以恢复此过程。

选择*停止删除对象*时，存储分段将返回到写入模式；但是，您无法访问或恢复已删除的任何对象。

6. 等待此操作完成。

   当存储分段为空时、状态横幅将更新、但存储分段仍保持只读状态。



7. 执行以下操作之一：

   - 退出页面以使存储分段保持只读模式。例如、您可以将一个空分段保留为只读模式、以保留该分段名称供将来使用。
   - 删除存储分段。您可以选择*删除存储分段*来删除单个存储分段，也可以返回“存储分段”页面并选择*操作*>*删除*存储分段来删除多个存储分段。

     > 如果在删除所有对象后无法删除分版本存储分段、则删除标记可能会保留下来。要删除存储分段、必须删除所有剩余的删除标记。

   - 将存储分段恢复为写入模式、并可选择将其用于新对象。您可以为单个存储分段选择*停止删除对象*，也可以返回到“存储分段”页面，并为多个存储分段选择*操作*>*停止删除对象*。

删除 S3 存储分段

您可以使用租户管理器删除一个或多个空的 S3 分段。

开始之前

- 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 "管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。
- 要删除的存储分段为空。

关于此任务

以下说明介绍如何使用租户管理器删除 S3 存储分段。您也可以使用删除 S3 存储分段 "租户管理 API" 或 "S3 REST API"。

如果S3存储分段包含对象、非当前对象版本或删除标记、则不能将其删除。有关如何删除S3版本对象的信息、请参阅 "如何删除对象"。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。

   此时将显示 " 分段 " 页面，其中会显示所有现有的 S3 分段。

2. 使用*操作*菜单或特定存储分段的详细信息页面。

   操作菜单

   a. 选中要删除的每个存储分段对应的复选框。

   b. 选择*Actions*>*Delete Buc分 段*。

   详细信息页面

   a. 选择存储分段名称以显示其详细信息。

   b. 选择*删除存储分段*。

3. 出现确认对话框时，选择*Yes*。

   StorageGRID 会确认每个存储分段均为空，然后删除每个存储分段。此操作可能需要几分钟时间。

   如果存储分段不为空，则会显示一条错误消息。必须先删除存储分段中的所有对象和任何删除标记、然后才能删除存储分段。

使用试验性 **S3** 控制台

您可以使用 S3 控制台查看 S3 存储分段中的对象。

您也可以使用 S3 控制台执行以下操作：

- 添加和删除对象，对象版本和文件夹
- 重命名对象
- 在分段和文件夹之间移动和复制对象
- 管理对象标记
- 查看对象元数据
- 下载对象

S3控制台标记为"试验性"、因为它尚未完成、或者尚未批准在生产环境中使用。只有在为少量对象执行功能时，租户才应使用 S3 控制台，例如上传对象以模拟新的 ILM 策略，排除载入问题或使用概念验证或非生产网格。

开始之前

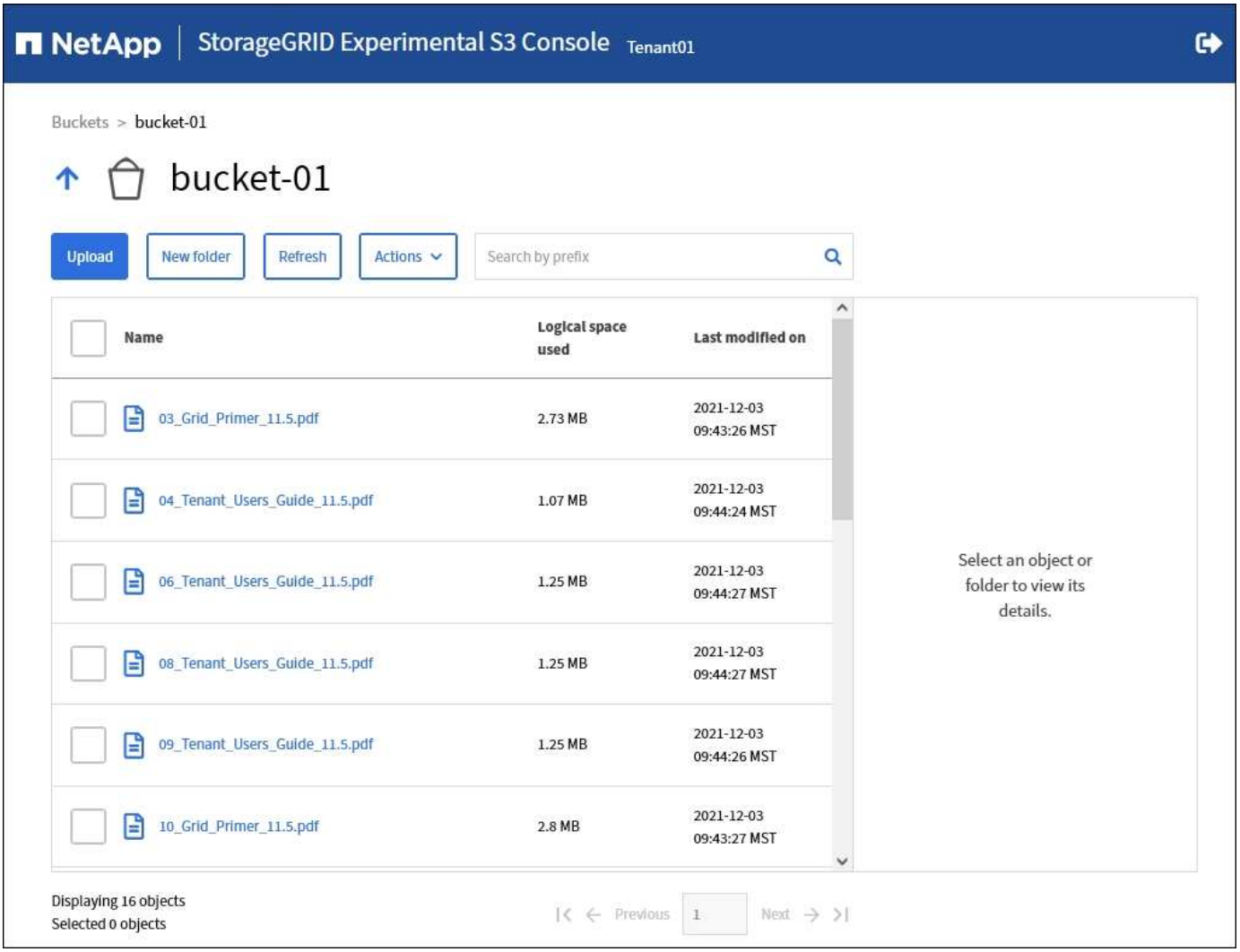
- 您将使用登录到租户管理器 "支持的 Web 浏览器"。
- 您所属的用户组具有root访问权限、或者同时具有"使用S3控制台管理所有分段"和"管理对象" "权限"。

> 具有"管理具有S3控制台"权限的对象但没有"管理所有分段"权限的用户仍可直接导航到"试行S3控制台"。

- 您已创建存储分段。
- 已为此用户配置S3组或存储分段策略。
- 您知道用户的访问密钥 ID 和机密访问密钥。(可选)您有 `.csv` 包含此信息的文件。请参见 "创建访问密钥的说明"。

步骤

1. 选择 * 分段 * 。
2. 选择 … Experimental S3 Console 。您也可以从存储分段详细信息页面访问此链接。
3. 在试验性 S3 控制台登录页面上，将访问密钥 ID 和机密访问密钥粘贴到字段中。否则，请选择*上传访问密钥*并选择您的 `.csv` 文件
4. 选择 * 登录 * 。
5. 根据需要管理对象。



管理 S3 平台服务

什么是平台服务?

StorageGRID 平台服务允许您向外部目标发送事件通知以及S3对象和对象元数据的副本、从而帮助您实施混合云战略。

如果您的租户帐户允许使用平台服务，则可以为任何 S3 存储分段配置以下服务：

- **CloudMirror**复制：使用 "StorageGRID CloudMirror 复制服务" 将特定对象从StorageGRID 存储分段镜像到指定的外部目标。

  例如，您可以使用 CloudMirror 复制将特定客户记录镜像到 Amazon S3 ，然后利用 AWS 服务对数据执行分析。

  > 如果源存储分段启用了 S3 对象锁定，则不支持 CloudMirror 复制。

- 通知：使用 "每个存储分段的事件通知" 将有关对对象执行的特定操作的通知发送到指定的外部Amazon Simple Notification Service™SNS。

例如，您可以配置向管理员发送有关添加到存储分段中的每个对象的警报，这些对象表示与关键系统事件关联的日志文件。

> 虽然可以在启用了 S3 对象锁定的存储分段上配置事件通知，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留至日期和合法保留状态）。

- 搜索集成服务：使用 "搜索集成服务" 将S3对象元数据发送到可使用外部服务在其中搜索或分析元数据的指定EI路径 搜索索引。

  例如，您可以将存储分段配置为将 S3 对象元数据发送到远程 Elasticsearch 服务。然后，您可以使用 Elasticsearch 跨存储分段执行搜索，并对对象元数据中存在的模式执行复杂的分析。

> 虽然可以在启用了 S3 对象锁定的情况下在存储分段上配置 Elasticsearch 集成，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留截止日期和合法保留状态）。

由于平台服务的目标位置通常不在 StorageGRID 部署中，因此平台服务可以为您提供使用外部存储资源，通知服务以及数据搜索或分析服务所带来的强大功能和灵活性。

可以为一个 S3 存储分段配置任何平台服务组合。例如，您可以在 StorageGRID S3 存储分段上配置 CloudMirror 服务和通知，以便将特定对象镜像到 Amazon Simple Storage Service ，同时向第三方监控应用程序发送有关每个此类对象的通知，以帮助您跟踪 AWS 支出。

> StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。

如何配置平台服务

平台服务可与您使用配置的外部端点进行通信 "租户管理器" 或 "租户管理 API"。每个端点都代表一个外部目标，例如 StorageGRID S3 存储分段， Amazon Web 服务分段，简单通知服务（ SNS ）主题或本地托管， AWS 或其他位置的 Elasticsearch 集群。

创建外部端点后、您可以通过向存储分段添加XML配置来为该存储分段启用平台服务。XML 配置可确定存储分段应处理的对象，存储分段应执行的操作以及存储分段应用于服务的端点。

您必须为要配置的每个平台服务添加单独的 XML 配置。例如：

- 所需的所有对象的密钥均以开头 `/images` 要复制到Amazon S3存储分段、您必须向源存储分段添加复制配置。
- 如果您还希望在这些对象存储到存储分段时发送通知，则必须添加通知配置。
- 最后，如果要为这些对象的元数据编制索引，则必须添加用于实施搜索集成的元数据通知配置。

配置 XML 的格式由用于实施 StorageGRID 平台服务的 S3 REST API 控制：

平台服务	**S3 REST API**
"CloudMirror 复制"	• 获取存储分段复制 • PUT 存储分段复制

平台服务	S3 REST API
"通知"	• 获取存储分段通知 • PUT 存储分段通知
"搜索集成"	• 获取存储分段元数据通知配置 • PUT 存储分段元数据通知配置 这些操作是 StorageGRID 的自定义操作。

相关信息

"平台服务注意事项"

"使用S3 REST API"

CloudMirror 复制服务

如果您希望 StorageGRID 将添加到 S3 存储分段的指定对象复制到一个或多个目标存储分段，则可以为该存储分段启用 CloudMirror 复制。

CloudMirror 复制独立于网格的活动 ILM 策略运行。CloudMirror 服务会在将对象存储到源存储分段时复制这些对象，并尽快将其交付到目标存储分段。对象载入成功后，系统将触发复制对象的传送。

CloudMirror复制与跨网格复制功能有重要的相似之处和不同之处。要了解更多信息，请参见 "请比较跨网格复制和CloudMirror复制"。

如果为现有存储分段启用 CloudMirror 复制，则只会复制添加到该存储分段的新对象。不会复制存储分段中的任何现有对象。要强制复制现有对象，您可以通过执行对象复制来更新现有对象的元数据。

如果您使用CloudMirror复制将对象复制到Amazon S3目标、请注意、Amazon S3会将每个Put请求标头中用户定义的元数据的大小限制为2 KB。如果对象的用户定义元数据大于 2 KB ，则不会复制该对象。

在 StorageGRID 中，您可以将单个存储分段中的对象复制到多个目标存储分段。为此，请为复制配置 XML 中的每个规则指定目标。不能同时将一个对象复制到多个分段。

此外，您还可以在受版本控制或未受版本控制的分段上配置 CloudMirror 复制，并可以指定受版本控制或未受版本控制的分段作为目标。您可以使用版本控制和未版本控制的分段的任意组合。例如，您可以将版本控制的存储分段指定为未版本控制的源存储分段的目标，反之亦然。您还可以在未版本控制的存储分段之间进行复制。

CloudMirror 复制服务的删除行为与 Amazon S3 提供的跨区域复制（ CRR ）服务的删除行为相同—删除源存储分段中的对象绝不会删除目标中的复制对象。如果源和目标存储分段都已进行版本控制，则会复制删除标记。如果目标分段未进行版本控制，则删除源分段中的对象不会将删除标记复制到目标分段或删除目标对象。

当对象复制到目标存储分段时， StorageGRID 会将其标记为 `replicas` 。 目标 StorageGRID 存储分段不会再次复制标记为副本的对象，从而防止意外复制环路。此副本标记是 StorageGRID 的内部标记，不会阻止您在使用 Amazon S3 存储分段作为目标时利用 AWS CRR 。

用于标记副本的自定义标头为 `x-ntap-sg-replica`。此标记可防止级联镜像。StorageGRID 支持在两个网格之间使用双向CloudMirror。

无法保证目标存储分段中事件的唯一性和顺序。由于为确保成功交付而执行的操作，可能会将一个源对象的多个相同副本传送到目标。在极少数情况下，如果从两个或更多不同的 StorageGRID 站点同时更新同一对象，则目标存储分段上的操作顺序可能与源存储分段上的事件顺序不匹配。

CloudMirror 复制通常配置为使用外部 S3 存储分段作为目标。但是，您也可以将复制配置为使用另一个 StorageGRID 部署或任何与 S3 兼容的服务。

了解存储分段通知

如果您希望 StorageGRID 向目标 Amazon Simple Notification Service （ SNS ）发送有关指定事件的通知，则可以为 S3 存储分段启用事件通知。

您可以 "配置事件通知" 通过将通知配置 XML 与源存储分段相关联。通知配置 XML 遵循 S3 配置存储分段通知的约定，并将目标 SNS 主题指定为端点的 URN 。

事件通知在通知配置中指定的源存储分段处创建，并传送到目标。如果与某个对象关联的事件成功，则会创建有关该事件的通知并排队等待传送。

不能保证通知的唯一性和顺序。由于为保证成功交付而执行的操作，可能会向目标发送多个事件通知。由于交付是异步的，因此无法保证目标上通知的时间顺序与源存储分段上事件的顺序一致，尤其是对于来自不同 StorageGRID 站点的操作。您可以使用 `sequencer` 键入事件消息以确定特定对象的事件顺序、如Amazon S3 文档中所述。

支持的通知和消息

StorageGRID 事件通知遵循Amazon S3 API、但存在一些限制：

- 支持以下事件类型：
  - S3：ObjectCreated：*
  - S3：对象创建：放置
  - S3：对象创建：发布
  - S3：对象创建：复制
  - S3：ObjectCreated：CompleteMultipartUpload
  - S3：ObjectRemoved：*
  - S3：ObjectRemoved：Delete
  - S3：ObjectRemoved：DeleteMarkerCreated
  - S3：ObjectRestore：POST
- 从StorageGRID 发送的事件通知使用标准JSON格式、但不包括某些密钥、而对其他密钥使用特定值、如表所示：

密钥名称	**StorageGRID** 值
事件源	`sgws:s3`
awsRegion	不包括
X-AMZ-ID-2	不包括
ARN	`urn:sgws:s3:::bucket_name`

了解搜索集成服务

如果要对对象元数据使用外部搜索和数据分析服务，则可以为 S3 存储分段启用搜索集成。

搜索集成服务是一种自定义 StorageGRID 服务，每当更新对象或其元数据时，该服务都会自动异步地将 S3 对象元数据发送到目标端点。然后，您可以使用目标服务提供的复杂搜索，数据分析，可视化或机器学习工具来搜索，分析对象数据并从中获得洞察力。

您可以为任何版本控制或未版本控制的存储分段启用搜索集成服务。搜索集成是通过将元数据通知配置 XML 与用于指定要对哪些对象执行操作的存储分段以及对象元数据的目标进行关联来配置的。

通知以 JSON 文档的形式生成，该文档使用分段名称，对象名称和版本 ID （如果有）命名。除了对象的所有标记和用户元数据之外，每个元数据通知还包含一组标准的对象系统元数据。

> 对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后、无法在索引中编辑文档的域类型。

每当出现以下情况时，都会生成通知并将其排队以供传送：

- 已创建对象。
- 删除对象，包括因网格的 ILM 策略操作而删除对象的时间。
- 添加，更新或删除对象元数据或标记。更新时始终会发送一组完整的元数据和标记，而不仅仅是更改后的值。

将元数据通知配置 XML 添加到存储分段后，系统会为您创建的任何新对象以及您通过更新其数据，用户元数据或标记来修改的任何对象发送通知。但是、不会为存储分段中已有的任何对象发送通知。要确保将存储分段中所有对象的对象元数据发送到目标，应执行以下任一操作：

- 创建存储分段后以及添加任何对象之前，请立即配置搜索集成服务。
- 对存储分段中已有的所有对象执行操作，此操作将触发元数据通知消息以发送到目标。

StorageGRID 搜索集成服务支持将 Elasticsearch 集群作为目标。与其他平台服务一样，目标也会在端点中指定，而此端点的 URN 会在该服务的配置 XML 中使用。使用 "NetApp 互操作性表工具" 确定支持的 Elasticsearch 版本。

相关信息

"用于搜索集成的配置 XML"

"元数据通知中包含的对象元数据"

"由搜索集成服务生成的 JSON"

"配置搜索集成服务"

平台服务注意事项

在实施平台服务之前，请查看有关使用这些服务的建议和注意事项。

有关 S3 的信息，请参见 "使用S3 REST API"。

使用平台服务的注意事项

注意事项	详细信息
目标端点监控	您必须监控每个目标端点的可用性。如果与目标端点的连接长时间断开，并且存在大量请求积压，则向 StorageGRID 发出的其他客户端请求（例如 PUT 请求）将失败。当端点可访问时，您必须重试这些失败的请求。
目标端点限制	如果发送请求的速率超过目标端点接收请求的速率， StorageGRID 软件可能会限制传入的存储分段 S3 请求。只有在等待发送到目标端点的请求积压时，才会发生限制。 唯一明显的影响是，传入的 S3 请求执行时间较长。如果您开始检测到性能明显较慢，则应降低载入速率或使用容量较高的端点。如果积压的请求持续增加，客户端 S3 操作（例如 PUT 请求）最终将失败。 CloudMirror 请求更有可能受到目标端点性能的影响，因为这些请求所涉及的数据传输通常多于搜索集成或事件通知请求。
订购担保	StorageGRID 保证对站点中的对象执行操作的顺序。只要针对某个对象的所有操作都位于同一站点内，最终对象状态（用于复制）就始终等于 StorageGRID 中的状态。 在跨 StorageGRID 站点执行操作时， StorageGRID 会尽力订购请求。例如，如果您先将某个对象写入站点 A ，然后覆盖站点 B 上的同一个对象，则 CloudMirror 复制到目标分段的最终对象不能保证为较新的对象。
ILM 驱动的对象删除	为了匹配AWS CRR和SNS服务的删除行为、在因StorageGRID ILM规则而删除源存储分段中的对象时、不会发送CloudMirror和事件通知请求。例如，如果 ILM 规则在 14 天后删除某个对象，则不会发送 CloudMirror 或事件通知请求。 相反，在因 ILM 而删除对象时，系统会发送搜索集成请求。

使用 **CloudMirror** 复制服务的注意事项

注意事项	详细信息
复制状态	StorageGRID 不支持 `x-amz-replication-status` 标题。
对象大小	CloudMirror 复制服务可复制到目标分段的对象的最大大小为 5 TiB ，与最大 _supported 对象大小相同。 • 注 * ：单个 PUT 对象操作的最大 _recommended_size 为 5 GiB （ 5 ， 368 ， 709 ， 120 字节）。如果对象大于 5 GiB ，请改用多部分上传。
存储分段版本控制和版本 ID	如果 StorageGRID 中的源 S3 存储分段已启用版本控制，则还应为目标存储分段启用版本控制。 使用版本控制时，请注意，由于 S3 协议的限制，在目标存储分段中排列对象版本是尽力而为的， CloudMirror 服务无法保证这一点。 注意：StorageGRID 中源存储分段的版本ID与目标存储分段的版本ID无关。
标记对象版本	由于 S3 协议的限制， CloudMirror 服务不会复制任何提供版本 ID 的 PUT 对象标记或删除对象标记请求。由于源和目标的版本ID不相关、因此无法确保复制对特定版本ID的标记更新。 相反、CloudMirror服务会复制Put对象标记请求或删除未指定版本ID的对象标记请求。这些请求会更新最新密钥的标记（如果分段已受版本控制，则更新最新版本的标记）。此外，还会复制具有标记（而不是标记更新）的常规载入。
多部分上传和 `ETag` values	镜像使用多部分上传方式上传的对象时， CloudMirror 服务不会保留这些部分。因此、将显示 `ETag` 镜像对象的值将与不同 `ETag` 原始对象的值。
使用 SSI-C 加密的对象（使用客户提供的密钥进行服务器端加密）	CloudMirror 服务不支持使用 SSI-C 加密的对象如果您尝试将对象载入源存储分段以进行 CloudMirror 复制，并且此请求包含 SSI-C 请求标头，则此操作将失败。
已启用 S3 对象锁定的存储分段	如果用于 CloudMirror 复制的目标 S3 存储分段已启用 S3 对象锁定，则配置存储分段复制（ PUT 存储分段复制）的尝试将失败，并显示 AccessDenied 错误。

配置平台服务端点

在为存储分段配置平台服务之前，必须至少将一个端点配置为平台服务的目标。

StorageGRID 管理员可以按租户访问平台服务。要创建或使用平台服务端点、您必须是具有"管理端点"或"根"访问权限的租户用户、并且网格中的网络连接已配置为允许存储节点访问外部端点资源。有关详细信息，请与 StorageGRID 管理员联系。

什么是平台服务端点?

创建平台服务端点时，您可以指定 StorageGRID 访问外部目标所需的信息。

例如、如果要将对象从StorageGRID 存储分段复制到Amazon S3存储分段、则需要创建一个平台服务端点、其中包含StorageGRID 访问Amazon上的目标存储分段所需的信息和凭据。

每种类型的平台服务都需要自己的端点，因此您必须为计划使用的每个平台服务至少配置一个端点。定义平台服务端点后，您可以在用于启用此服务的配置 XML 中使用此端点的 URN 作为目标。

您可以对多个源存储分段使用与目标相同的端点。例如，您可以配置多个源分段，将对象元数据发送到同一搜索集成端点，以便可以跨多个分段执行搜索。您还可以将源分段配置为使用多个端点作为目标，这样您可以执行以下操作：向一个 SNS 主题发送有关对象创建的通知，向另一个 SNS 主题发送有关对象删除的通知。

用于 **CloudMirror** 复制的端点

StorageGRID 支持表示 S3 存储分段的复制端点。这些存储分段可能托管在 Amazon Web Services ，相同或远程 StorageGRID 部署或其他服务上。

通知的端点

StorageGRID 支持简单通知服务（ SNS ）端点。不支持简单队列服务(Simple Queue Service、SQS)或AWS Lamba端点。

搜索集成服务的端点

StorageGRID 支持表示 Elasticsearch 集群的搜索集成端点。这些EI路径 搜索集群可以位于本地数据中心、也可以托管在AWS云或其他位置。

搜索集成端点是指特定的 Elasticsearch 索引和类型。您必须先在 Elasticsearch 中创建索引，然后才能在 StorageGRID 中创建端点，否则端点创建将失败。在创建端点之前、无需创建类型。如果需要， StorageGRID 将在向端点发送对象元数据时创建此类型。

相关信息

"管理 StorageGRID"

为平台服务端点指定 **URN**

创建平台服务端点时，必须指定唯一资源名称（ URN ）。在为平台服务创建配置 XML 时，您将使用 URN 引用此端点。每个端点的 URN 必须是唯一的。

StorageGRID 会在您创建平台服务端点时对其进行验证。在创建平台服务端点之前，请确认此端点中指定的资源存在且可访问。

urn 元素

平台服务端点的URN必须以任一开头 `arn:aws` 或 `urn:mysite`、如下所示：

- 如果服务托管在Amazon Web Services (AWS)上、请使用 `arn:aws`。
- 如果服务托管在Google Cloud Platform (GCP)上、请使用 `arn:aws`。
- 如果服务托管在本地、请使用 `urn:mysite`

例如、如果要为StorageGRID 上托管的CloudMirror端点指定URN、则URN可能以开头 `urn:sgws`。

URN 的下一个元素用于指定平台服务的类型，如下所示：

服务	Type
CloudMirror 复制	S3
通知	SnS
搜索集成	ES

例如、要继续为StorageGRID 上托管的CloudMirror端点指定URN、您需要添加 `s3` 获取 `urn:sgws:s3`。

URN 的最后一个元素用于标识目标 URI 上的特定目标资源。

服务	特定资源
CloudMirror 复制	分段名称
通知	Sns-topic-name
搜索集成	`domain-name/index-name/type-name` • 注意： * 如果 Elasticsearch 集群已配置为 * 不 * 自动创建索引，则必须在创建端点之前手动创建索引。

AWS 和 GCP 上托管的服务的 urns

对于 AWS 和 GCP 实体，完整的 URN 是有效的 AWS ARN 。例如：

- CloudMirror 复制：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 搜索集成：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

对于AWS搜索集成端点、为 `domain-name` 必须包含文字字符串 `domain/`、如下所示。

用于本地托管服务的 **urns**

使用本地托管的服务而非云服务时，只要 URN 在第三个和最后一个位置包含所需的元素，您就可以以任何方式指定 URN 以创建有效且唯一的 URN 。您可以将可选元素留空，也可以通过任何方式指定这些元素，以帮助您标识资源并使 URN 具有唯一性。例如：

- CloudMirror 复制：

```
urn:mysite:s3:optional:optional:bucket-name
```

对于StorageGRID 上托管的CloudMirror端点、您可以指定以开头的有效URN `urn:sgws`：

```
urn:sgws:s3:optional:optional:bucket-name
```

- 通知：

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- 搜索集成：

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> 对于本地托管的搜索集成端点、为 `domain-name` 只要端点的URN是唯一的、Element就可以是任意字符串。

创建平台服务端点

必须至少创建一个正确类型的端点，然后才能启用平台服务。

开始之前

- 您将使用登录到租户管理器 "支持的 Web 浏览器"。
- StorageGRID 管理员已为租户帐户启用平台服务。
- 您属于具有的用户组 "管理端点或root访问权限"。
- 已创建平台服务端点引用的资源：
  - CloudMirror 复制： S3 存储分段
  - 事件通知： SnS 主题
  - 搜索通知： Elasticsearch index ，如果目标集群未配置为自动创建索引。
- 您知道有关目标资源的信息：
  - 统一资源标识符（ URI ）的主机和端口

如果您计划使用 StorageGRID 系统上托管的存储分段作为 CloudMirror 复制的端点，请联系网格管理员以确定需要输入的值。

- 唯一资源名称（ URN ）

  "为平台服务端点指定 URN"

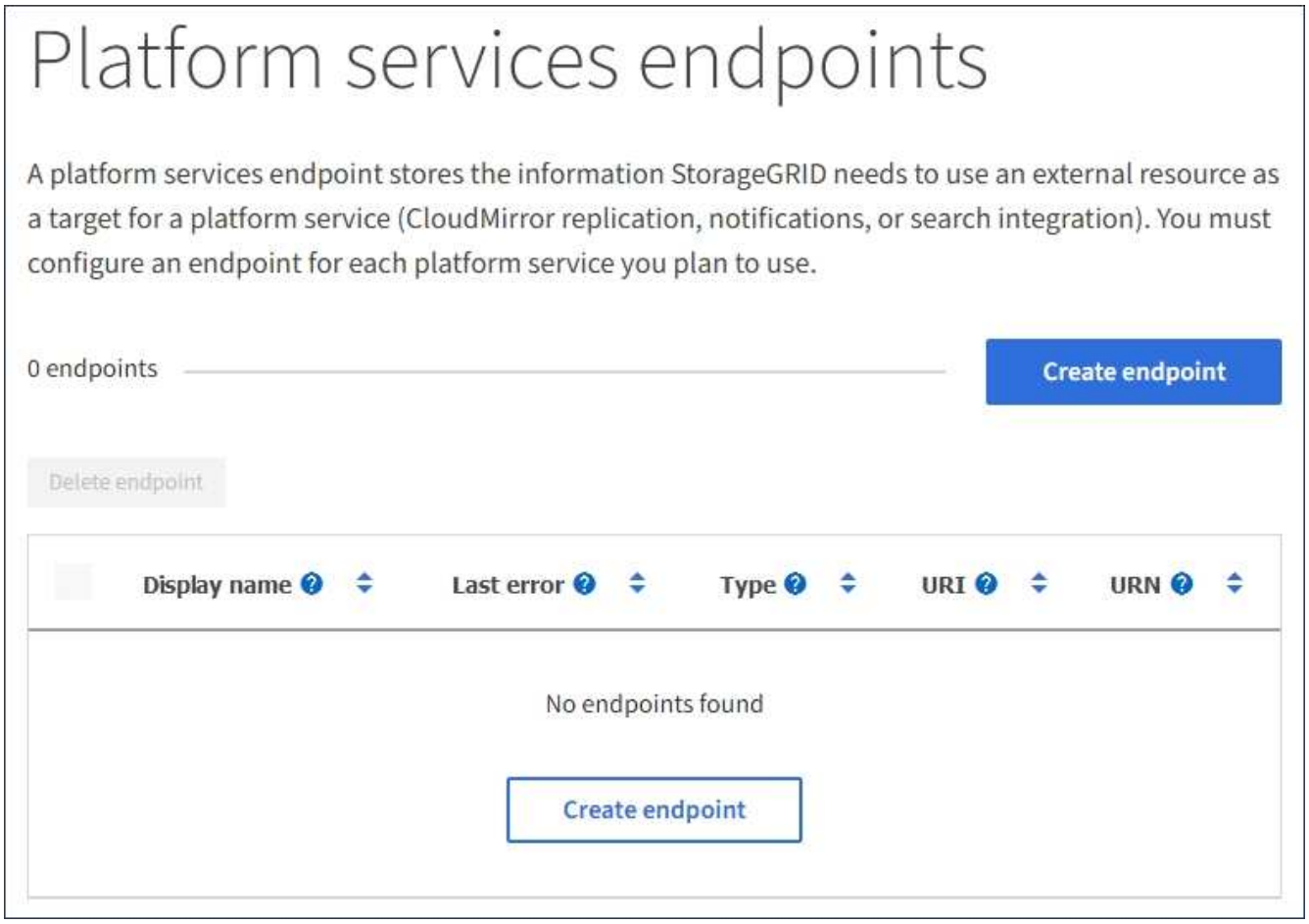
- 身份验证凭据（如果需要）：
  - 访问密钥：访问密钥 ID 和机密访问密钥
  - 基本 HTTP ： 用户名和密码
  - CAP （ C2S 访问门户）： 临时凭据 URL ，服务器和客户端证书，客户端密钥以及可选的客户端专用密钥密码短语。
- 安全证书（如果使用自定义 CA 证书）

- 如果启用了EI在任 一EI在任 一安全功能中、您将拥有用于连接测试的监控集群权限、以及用于文档更新的写入索引权限或同时具有索引和删除索引权限。

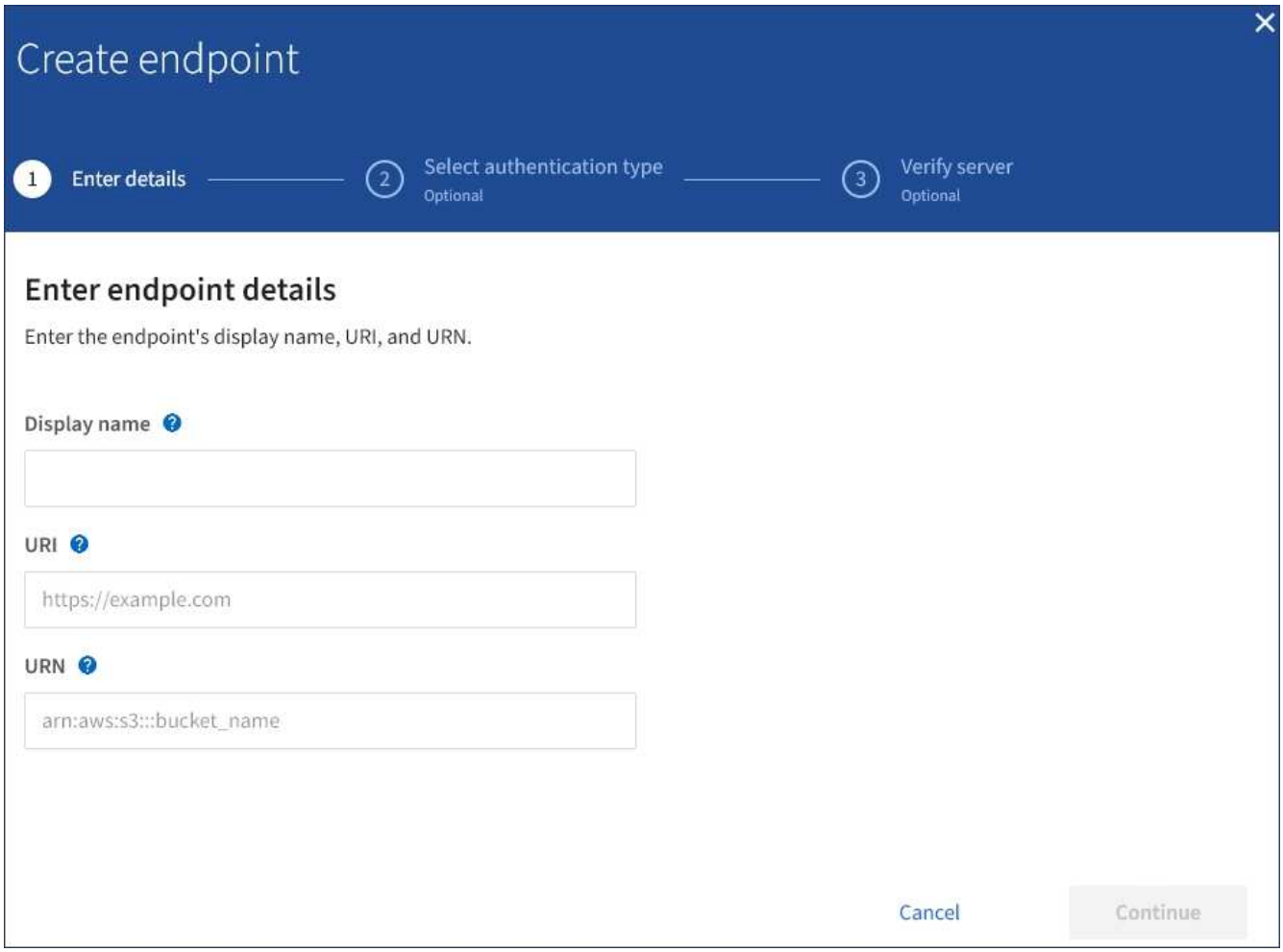
步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面。



2. 选择 * 创建端点 * 。



3. 输入显示名称以简要说明端点及其用途。

   当端点名称在"端点"页面上列出时、端点支持的平台服务类型显示在端点名称旁边、因此您无需在名称中包含该信息。

4. 在 * URI * 字段中，指定端点的唯一资源标识符（ URI ）。

   请使用以下格式之一：

   ```
   https://host:port
   http://host:port
   ```

   如果未指定端口、则端口443用于HTTPS URL、端口80用于HTTP URL。

   例如， StorageGRID 上托管的存储分段的 URI 可能为：

   ```
   https://s3.example.com:10443
   ```

   在此示例中、 `s3.example.com` 表示StorageGRID 高可用性(HA)组的虚拟IP (VIP)和的DNS条目 `10443` 表示在负载平衡器端点中定义的端口。

应尽可能连接到负载平衡节点的HA组、以避免单点故障。

同样， AWS 上托管的存储分段的 URI 可能为：

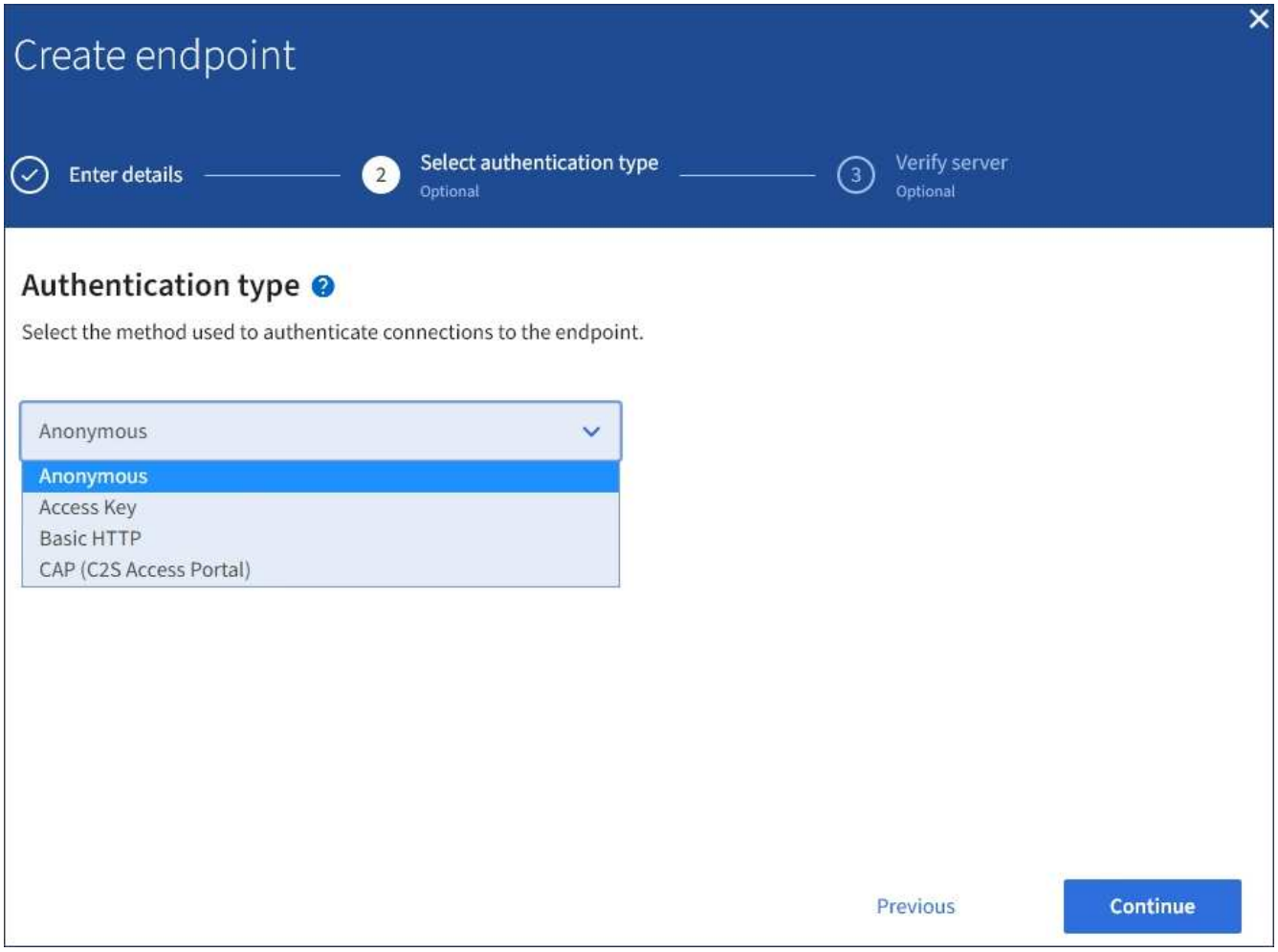
```
https://s3-aws-region.amazonaws.com
```

如果此端点用于CloudMirror复制服务、请勿在URI中包含存储分段名称。您可以在 * URN* 字段中包含分段名称。

5. 输入端点的唯一资源名称（ URN ）。

创建端点后、您无法更改此端点的URN。

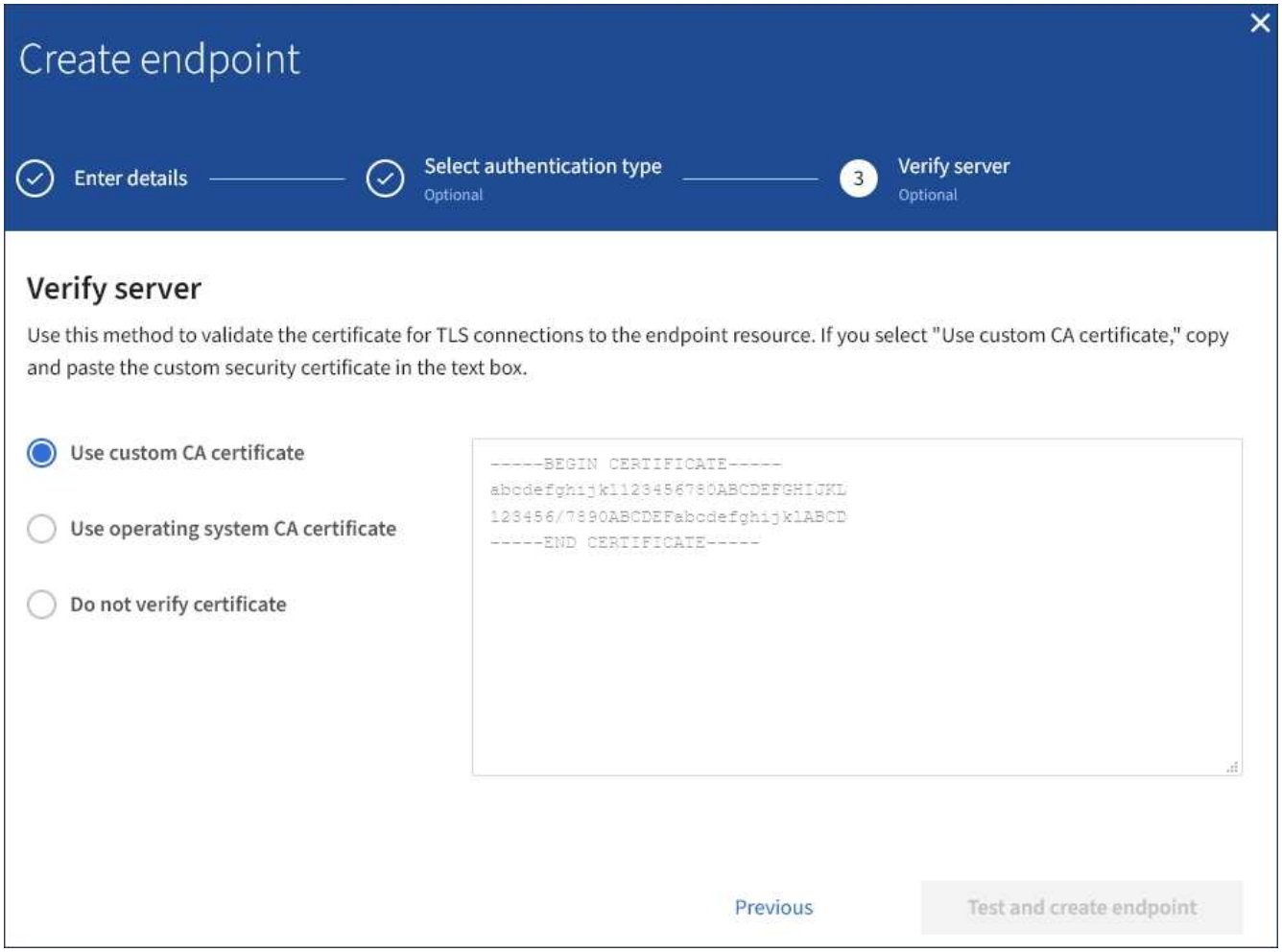
6. 选择 * 继续 * 。
7. 为 * 身份验证类型 * 选择一个值，然后输入或上传所需的凭据。



您提供的凭据必须具有目标资源的写入权限。

Authentication type	Description	凭据
匿名	提供对目标的匿名访问。仅适用于已禁用安全性的端点。	无身份验证。
访问密钥	使用 AWS 模式的凭据对与目标的连接进行身份验证。	• 访问密钥 ID • 机密访问密钥
基本 HTTP	使用用户名和密码对目标连接进行身份验证。	• Username • Password
CAP （ C2S 访问门户）	使用证书和密钥对目标连接进行身份验证。	• 临时凭据 URL • 服务器 CA 证书（ PEM 文件上传） • 客户端证书（ PEM 文件上传） • 客户端专用密钥（ PEM 文件上传，OpenSSL 加密格式或未加密的专用密钥格式） • 客户端专用密钥密码短语（可选）

8. 选择 * 继续 * 。
9. 选择 * 验证服务器 * 单选按钮以选择如何验证与端点的 TLS 连接。



证书验证的类型	Description
使用自定义 CA 证书	使用自定义安全证书。如果选择此设置，请在 * CA 证书 * 文本框中复制并粘贴自定义安全证书。
使用操作系统 CA 证书	使用操作系统上安装的默认网格 CA 证书来保护连接。
请勿验证证书	未验证用于 TLS 连接的证书。此选项不安全。

10. 选择 * 测试并创建端点 * 。
    - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
    - 如果端点验证失败，则会显示一条错误消息。如果需要修改端点以更正错误，请选择 * 返回到端点详细信息 * 并更新此信息。然后，选择 * 测试并创建端点 * 。

    如果未为租户帐户启用平台服务、则端点创建将失败。请与 StorageGRID 管理员联系。

配置端点后，您可以使用其 URN 配置平台服务。

相关信息

"为平台服务端点指定 URN"

"配置 CloudMirror 复制"

"配置事件通知"

"配置搜索集成服务"

测试平台服务端点的连接

如果与平台服务的连接发生更改，您可以测试端点的连接，以验证目标资源是否存在以及是否可以使用您指定的凭据访问它。

开始之前

- 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 "管理端点或root访问权限"。

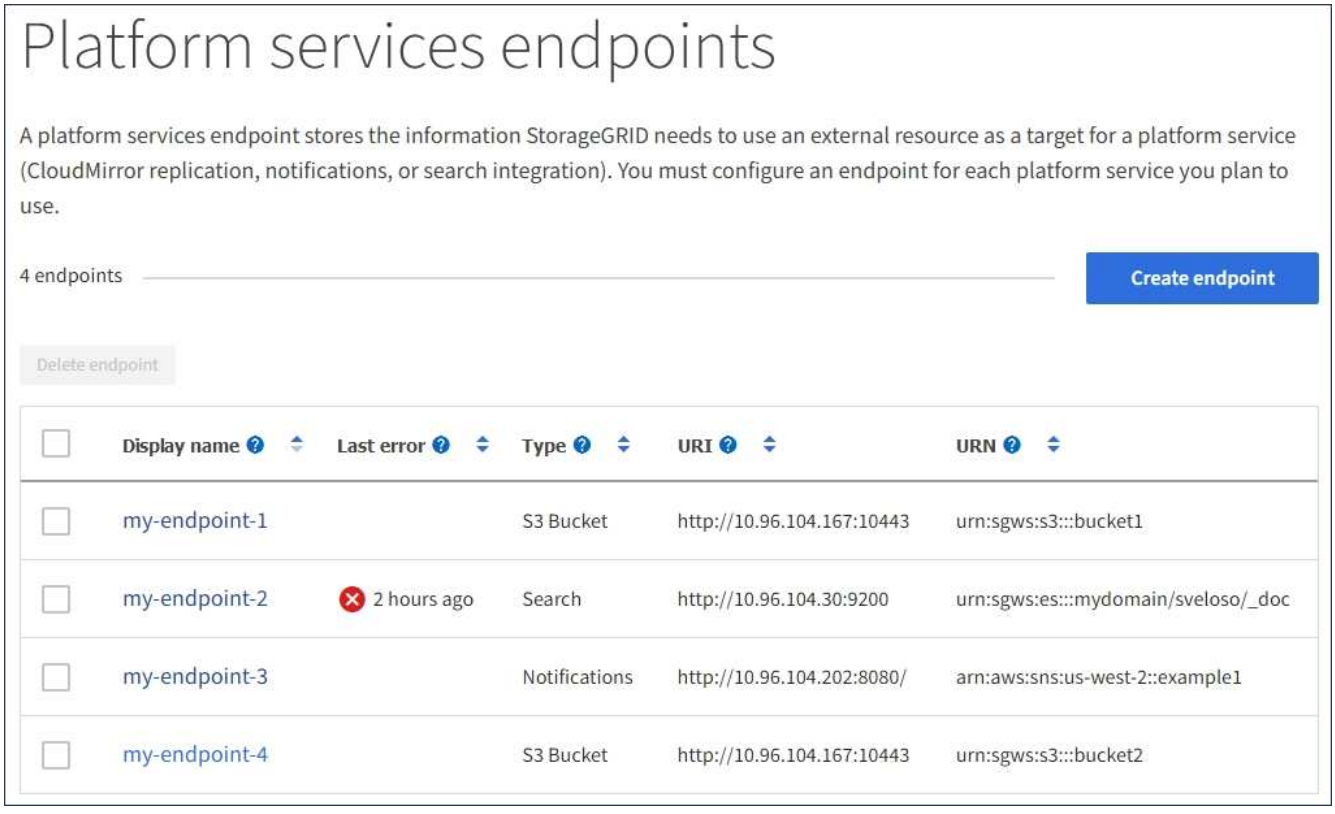
关于此任务

StorageGRID 不会验证这些凭据是否具有正确的权限。

步骤

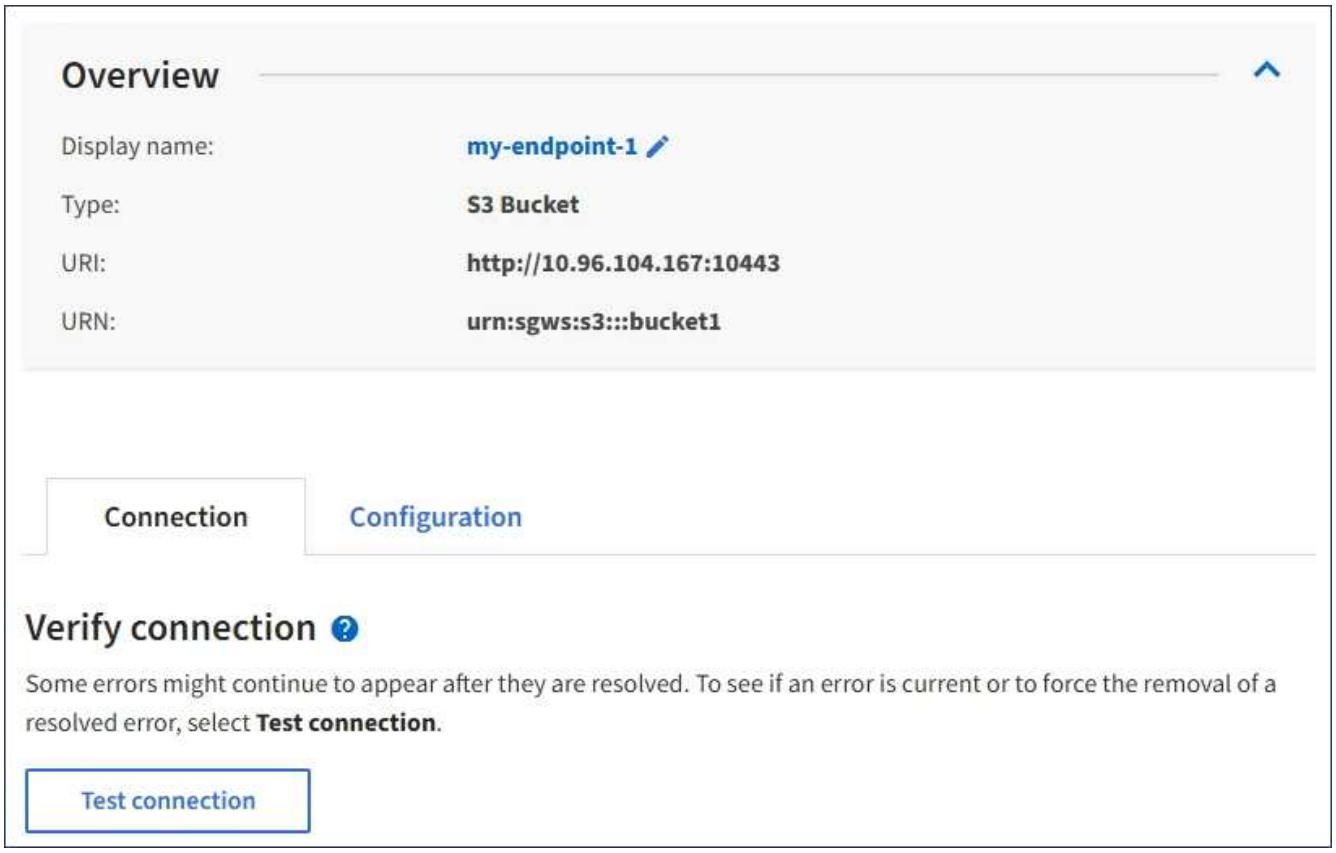
1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。



2. 选择要测试其连接的端点。

此时将显示端点详细信息页面。



3. 选择 * 测试连接 * 。
   - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
   - 如果端点验证失败，则会显示一条错误消息。如果需要修改端点以更正错误，请选择 * 配置 * 并更新信息。然后，选择 * 测试并保存更改 * 。

编辑平台服务端点

您可以编辑平台服务端点的配置以更改其名称， URI 或其他详细信息。例如，您可能需要更新已过期的凭据或更改 URI 以指向备份 Elasticsearch 索引以进行故障转移。您不能更改平台服务端点的URN。

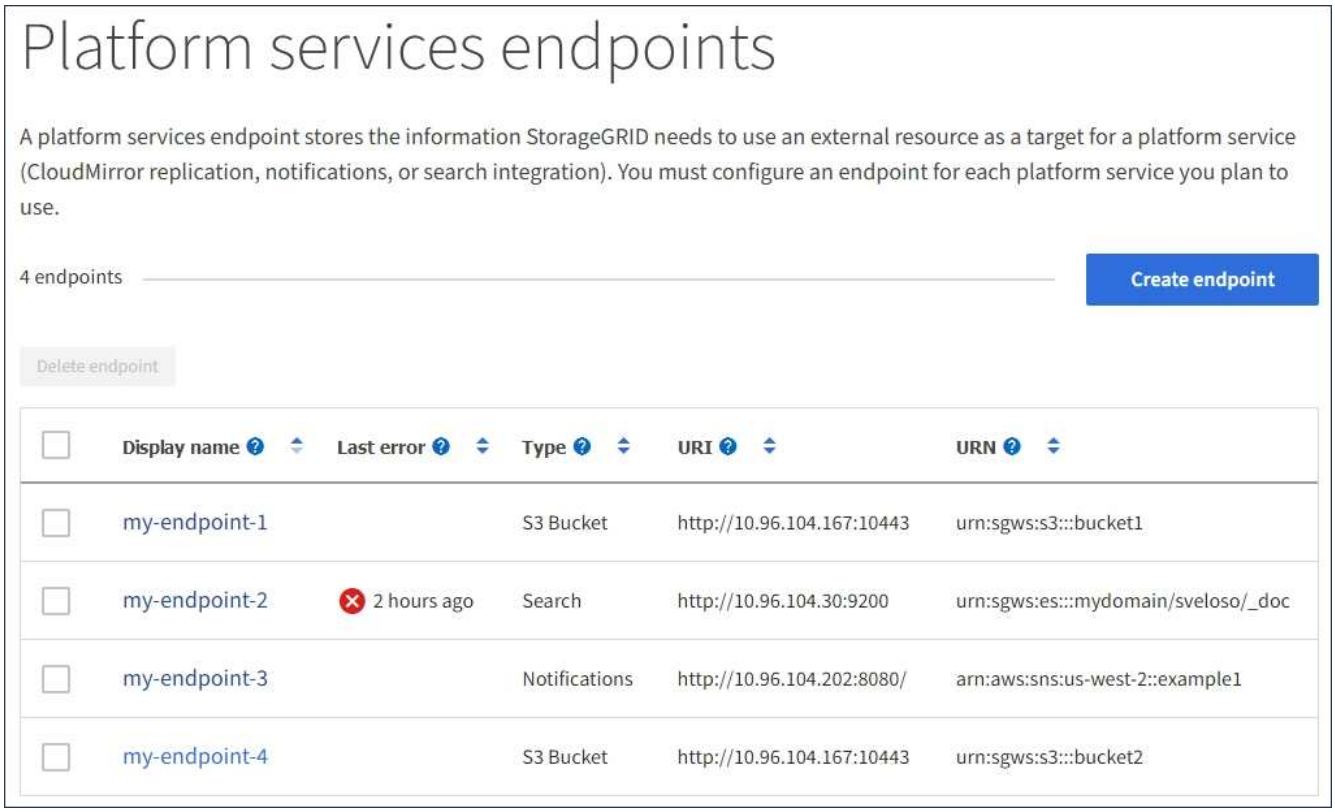
开始之前

- 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 "管理端点或root访问权限"。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

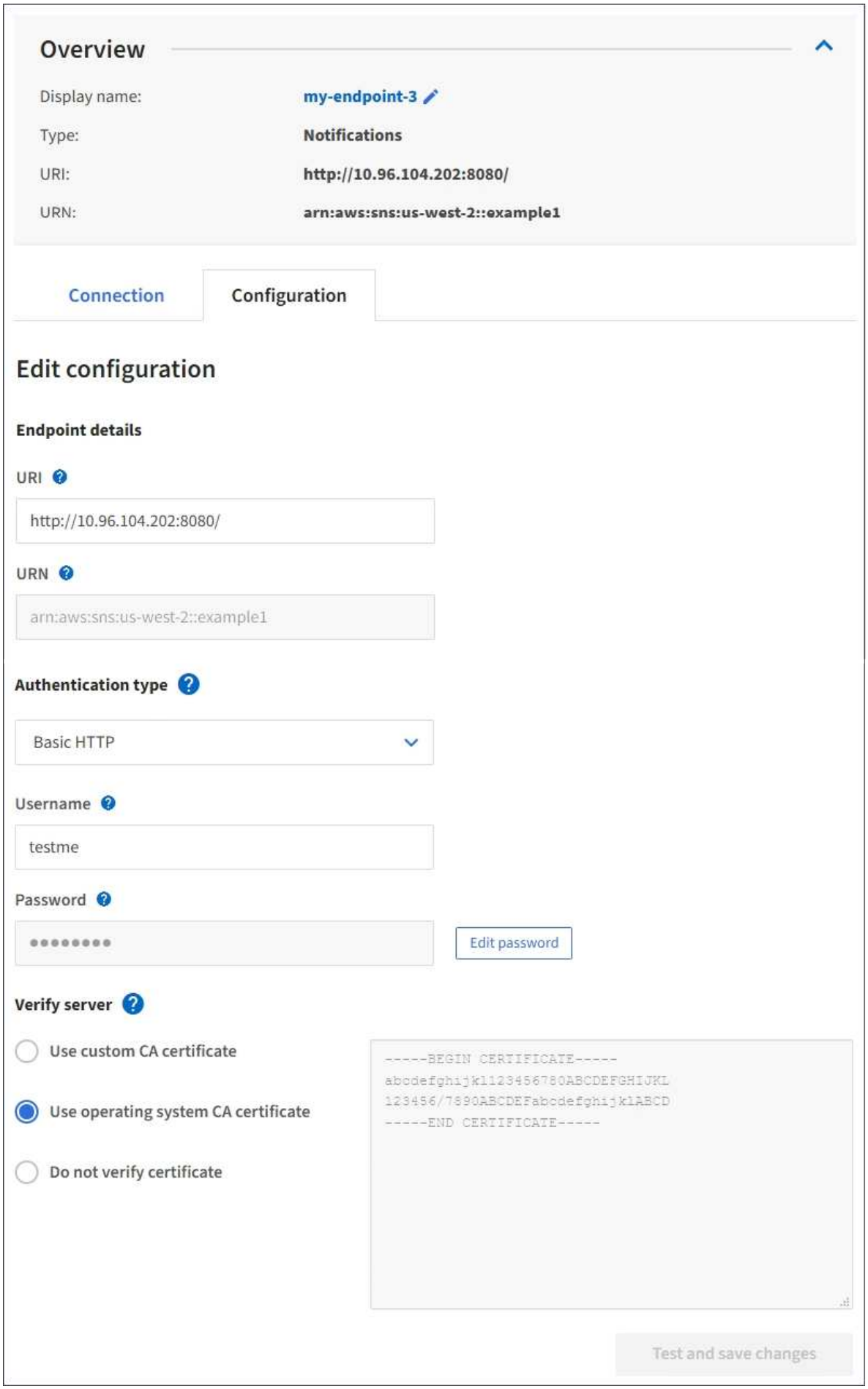
   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。



2. 选择要编辑的端点。

   此时将显示端点详细信息页面。

3. 选择 * 配置 * 。


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. 根据需要更改端点的配置。

   创建端点后、您无法更改此端点的URN。

   a. 要更改端点的显示名称，请选择编辑图标 。

   b. 根据需要更改 URI 。

   c. 根据需要更改身份验证类型。

      - 对于访问密钥身份验证，请根据需要更改密钥，方法是选择 * 编辑 S3 密钥 * 并粘贴新的访问密钥 ID 和机密访问密钥。如果需要取消所做的更改，请选择 * 还原 S3 密钥编辑 * 。
      - 对于基本 HTTP 身份验证，请根据需要更改用户名。根据需要更改密码，方法是选择 * 编辑密码 * 并输入新密码。如果需要取消所做的更改，请选择 * 还原密码编辑 * 。
      - 对于 CAP （ C2S 访问门户）身份验证，更改临时凭据 URL 或可选客户端专用密钥密码短语，并根据需要上传新的证书和密钥文件。

        客户端专用密钥必须采用 OpenSSL 加密格式或未加密的专用密钥格式。

   d. 根据需要更改用于验证服务器的方法。

5. 选择 * 测试并保存更改 * 。

   - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
   - 如果端点验证失败，则会显示一条错误消息。修改端点以更正错误，然后选择 * 测试并保存更改 * 。

删除平台服务端点

如果您不想再使用关联的平台服务，可以删除端点。

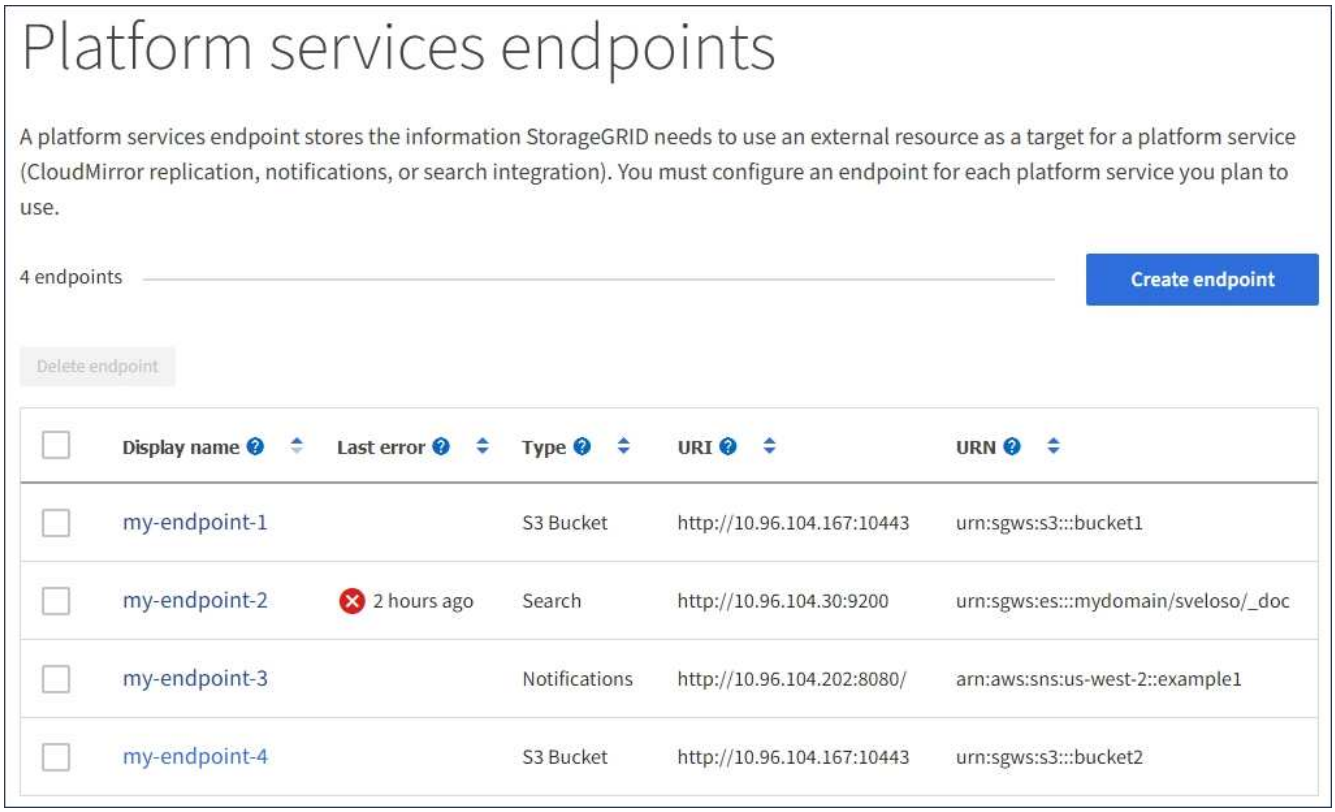
开始之前

- 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 "管理端点或root访问权限"。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。

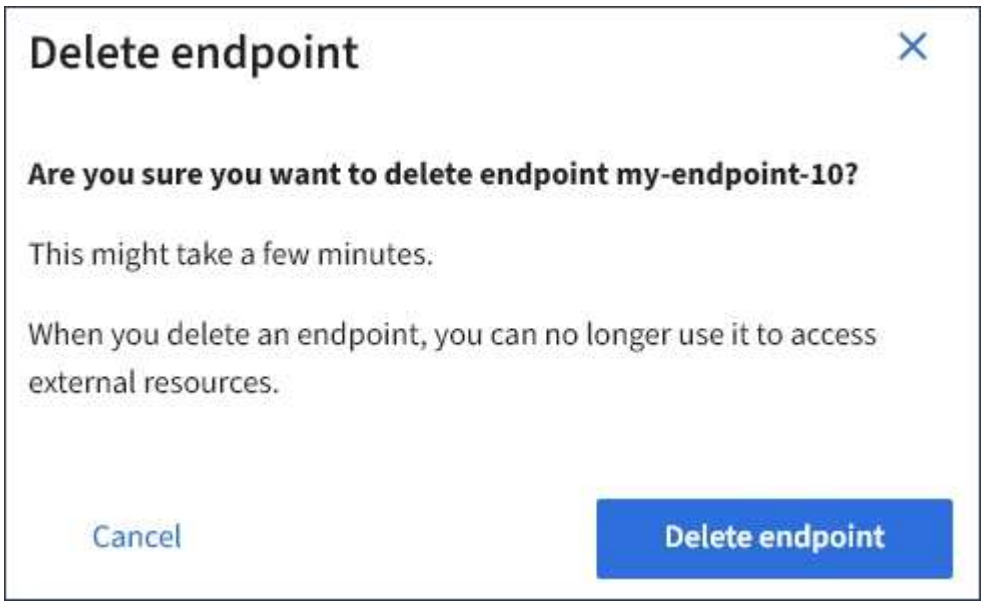


2. 选中要删除的每个端点对应的复选框。

> 如果删除正在使用的平台服务端点，则使用此端点的任何分段都将禁用关联的平台服务。任何尚未完成的请求都将被丢弃。所有新请求都将继续生成，直到您更改存储分段配置以不再引用已删除的 URN 为止。StorageGRID 会将这些请求报告为不可恢复的错误。

3. 选择 * 操作 * > * 删除端点 * 。

此时将显示一条确认消息。

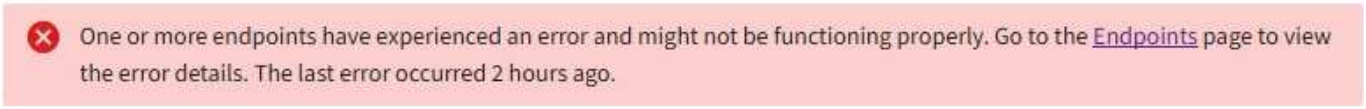


4. 选择 * 删除端点 * 。

如果在StorageGRID 尝试与平台服务端点通信时发生错误、则信息板上会显示一条消息。在平台服务端点页面上，最后一个错误列指示错误发生多长时间前。如果与端点凭据关联的权限不正确，则不会显示任何错误。

确定是否发生错误

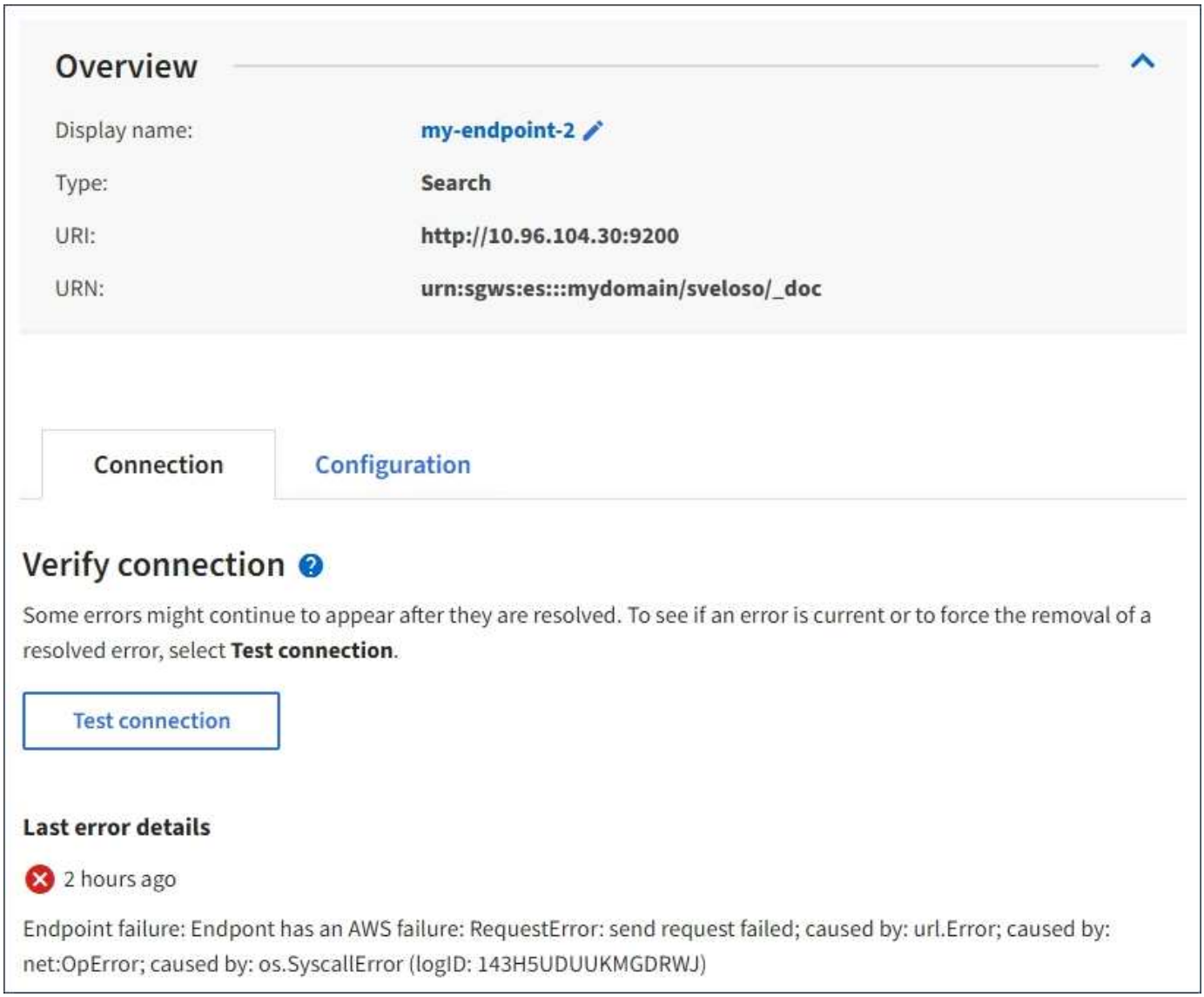
如果在过去7天内发生任何平台服务端点错误、租户管理器信息板将显示警报消息。您可以转到平台服务端点页面以查看有关此错误的更多详细信息。



信息板上显示的同一错误也会显示在平台服务端点页面的顶部。要查看更详细的错误消息，请执行以下操作：

步骤

1. 从端点列表中，选择出现错误的端点。
2. 在端点详细信息页面上，选择 * 连接 * 。此选项卡仅显示端点的最新错误，并指示错误发生的时间。包含红色 X 图标的错误 发生在过去 7 天内。



检查错误是否仍然是最新的

即使解决了某些错误， * 最后一个错误 * 列也可能会继续显示这些错误。要查看错误是否为当前错误或强制从表中删除已解决的错误，请执行以下操作：

步骤

1. 选择端点。

   此时将显示端点详细信息页面。

2. 选择 * 连接 * > * 测试连接 * 。

选择 * 测试连接 * 将使 StorageGRID 验证平台服务端点是否存在以及是否可以使用当前凭据访问它。系统会从每个站点的一个节点验证与端点的连接。

解决端点错误

您可以使用端点详细信息页面上的 * 最后一个错误 * 消息来帮助确定导致错误的原因。某些错误可能需要编辑端点才能解决问题描述 。例如，如果 StorageGRID 由于没有正确的访问权限或访问密钥已过期而无法访问目标 S3 存储分段，则可能会发生 CloudMirrorbuc2 错误。消息为 "`需要更新端点凭据或目标访问，` " ，详细信息为

"`AccessDenied` " 或 "`InvalidAccessKeyId 。` "

如果您需要编辑端点以解决错误，则选择 * 测试并保存更改 * 会使 StorageGRID 验证更新后的端点，并确认可以使用当前凭据访问它。系统会从每个站点的一个节点验证与端点的连接。

步骤

1. 选择端点。
2. 在端点详细信息页面上，选择 * 配置 * 。
3. 根据需要编辑端点配置。
4. 选择 * 连接 * > * 测试连接 * 。

权限不足的端点凭据

当 StorageGRID 验证平台服务端点时，它会确认端点的凭据可用于联系目标资源，并执行基本权限检查。但是， StorageGRID 不会验证某些平台服务操作所需的所有权限。因此，如果您在尝试使用平台服务（例如 "`403 For禁用` " ）时收到错误，请检查与此端点凭据关联的权限。

相关信息

- "管理StorageGRID ()；对平台服务进行故障排除"
- "创建平台服务端点"
- "测试平台服务端点的连接"
- "编辑平台服务端点"

配置 CloudMirror 复制

。 "CloudMirror 复制服务" 是三种 StorageGRID 平台服务之一。您可以使用 CloudMirror 复制将对象自动复制到外部 S3 存储分段。

开始之前

- StorageGRID 管理员已为租户帐户启用平台服务。
- 您已创建一个存储分段以用作复制源。
- 要用作CloudMirror复制目标的端点已存在、并且您具有其URN。
- 您属于具有的用户组 "管理所有分段或root访问权限"。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

CloudMirror 复制会将对象从源存储分段复制到端点中指定的目标存储分段。

CloudMirror复制与跨网格复制功能有重要的相似之处和不同之处。要了解更多信息，请参见 "请比较跨网格复制和CloudMirror复制"。

要为存储分段启用 CloudMirror 复制，必须创建并应用有效的存储分段复制配置 XML 。复制配置 XML 必须对每个目标使用 S3 存储分段端点的 URN 。

启用了 S3 对象锁定的源或目标分段不支持复制。

有关存储分段复制以及如何配置的常规信息、请参见 "Amazon Simple Storage Service (S3)文档：复制对象"。有关StorageGRID 如何实施GetBucketReplication、DeleteBucketReplication和PutBucketReplication的信息、请参见 "对存储分段执行的操作"。

如果在包含对象的存储分段上启用CloudMirror复制、则会复制添加到该存储分段的新对象、但不会复制该存储分段中的现有对象。您必须更新现有对象才能触发复制。

如果在复制配置 XML 中指定存储类，则 StorageGRID 在对目标 S3 端点执行操作时会使用该类。目标端点还必须支持指定的存储类。请务必遵循目标系统供应商提供的任何建议。

步骤

1. 为源存储分段启用复制：

   使用文本编辑器创建在 S3 复制 API 中指定的启用复制所需的复制配置 XML 。配置 XML 时：

   - 请注意， StorageGRID 仅支持复制配置的 V1 。这意味着、StorageGRID 不支持使用 `Filter` Element 中的规则、并遵循V1中有关删除对象版本的约定。有关详细信息，请参见有关复制配置的 Amazon 文档。
   - 使用 S3 存储分段端点的 URN 作为目标。
   - 也可以添加 `<StorageClass>` 元素、并指定以下项之一：
     - `STANDARD`：默认存储类。如果在上传对象时未指定存储类、则为 `STANDARD` 已使用存储类。
     - `STANDARD_IA`：(标准—不常访问。)对于访问频率较低但仍需要在需要时快速访问的数据、请使用此存储类。
     - `REDUCED_REDUNDANCY`：将此存储类用于存储冗余程度低于的非关键、可重现的数据 `STANDARD` 存储类。
   - 如果指定 `Role` 在配置XML中、此参数将被忽略。StorageGRID 不使用此值。

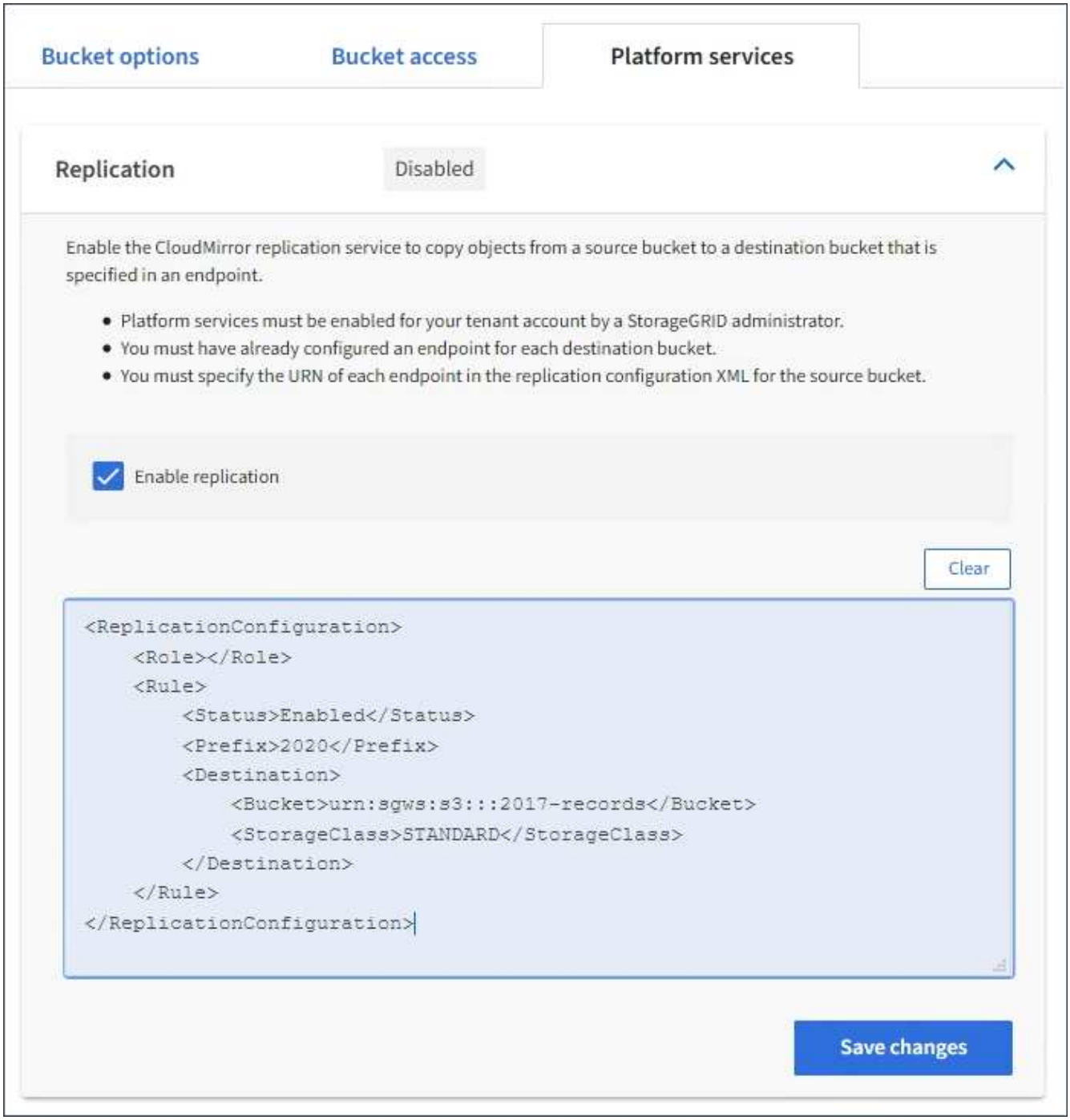
   ```
   <ReplicationConfiguration>
       <Role></Role>
       <Rule>
           <Status>Enabled</Status>
           <Prefix>2020</Prefix>
           <Destination>
              <Bucket>urn:sgws:s3:::2017-records</Bucket>
              <StorageClass>STANDARD</StorageClass>
            </Destination>
        </Rule>
   </ReplicationConfiguration>
   ```

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. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 复制 * 。

5. 选中*启用复制*复选框。
6. 将复制配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。



StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证复制配置是否正确：
   a. 向源存储分段添加一个对象，以满足复制配置中指定的复制要求。

      在前面显示的示例中，复制与前缀 "`2020` " 匹配的对象。

b. 确认对象已复制到目标存储分段。

对于小型对象，复制操作会快速进行。

相关信息

"创建平台服务端点"

配置事件通知

通知服务是三种 StorageGRID 平台服务之一。您可以为存储分段启用通知，以便将有关指定事件的信息发送到支持 AWS Simple Notification Service （ SNS ）的目标服务。

开始之前

- StorageGRID 管理员已为租户帐户启用平台服务。
- 您已创建一个存储分段来用作通知源。
- 要用作事件通知目标的端点已存在、并且您具有其URN。
- 您属于具有的用户组 "管理所有分段或root访问权限"。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

配置事件通知后，每当源存储分段中的某个对象发生指定事件时，都会生成一个通知，并将其发送到用作目标端点的简单通知服务（ SNS ）主题。要为存储分段启用通知，必须创建并应用有效的通知配置 XML 。通知配置 XML 必须使用每个目标的事件通知端点的 URN 。

有关事件通知以及如何配置这些通知的常规信息、请参见亚马逊文档。有关StorageGRID 如何实施S3存储分段通知配置API的信息、请参见有关实施S3客户端应用程序的说明。

如果为包含对象的存储分段启用事件通知，则仅会为保存通知配置后执行的操作发送通知。

步骤

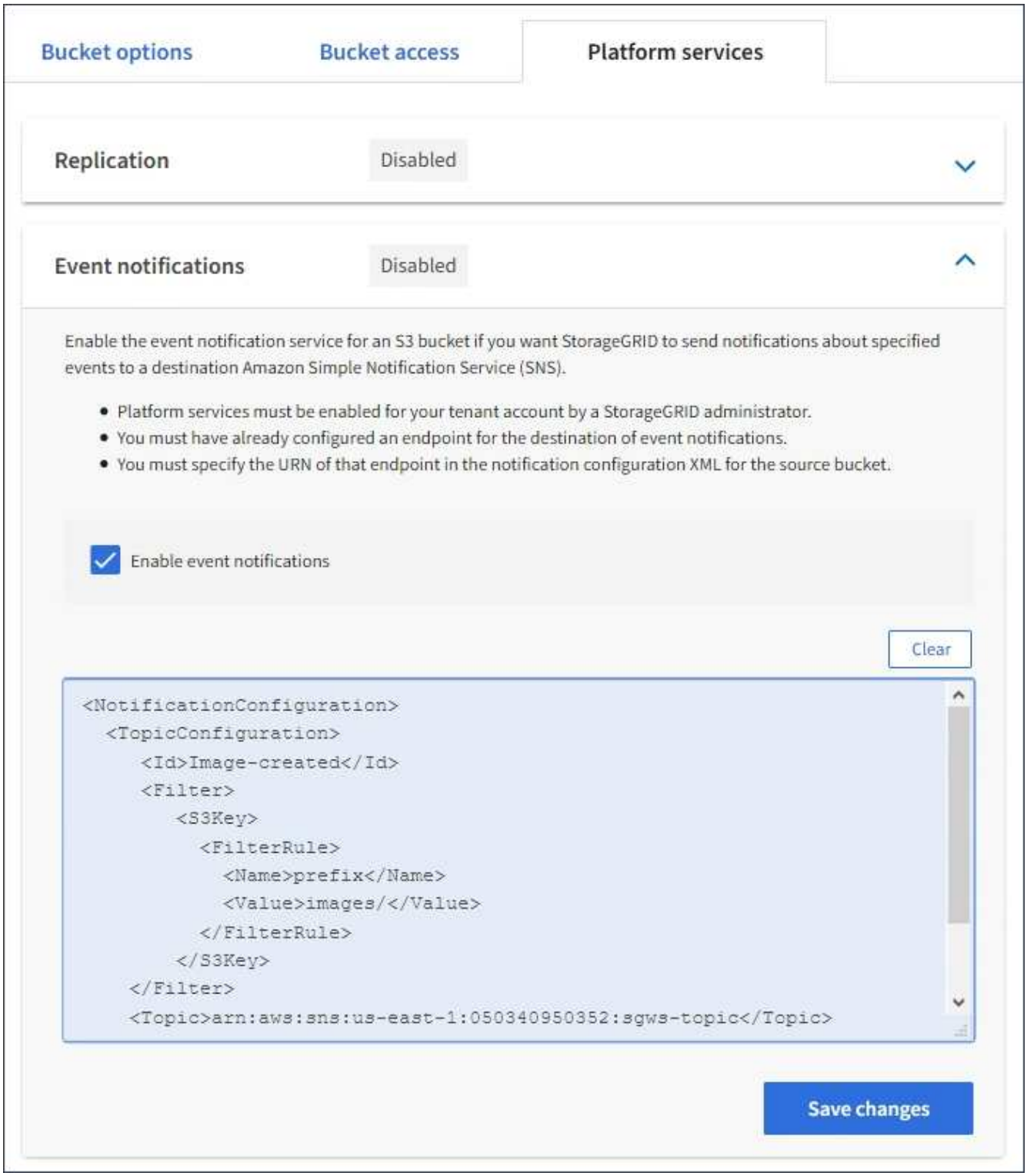
1. 为源存储分段启用通知：
    - 使用文本编辑器创建启用 S3 通知 API 中指定的事件通知所需的通知配置 XML 。
    - 配置 XML 时，请使用事件通知端点的 URN 作为目标主题。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 事件通知 * 。
5. 选中*启用事件通知*复选框。
6. 将通知配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。



StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证是否已正确配置事件通知：

   a. 对源存储分段中符合配置 XML 中配置的触发通知要求的对象执行操作。

      在此示例中、每当使用创建对象时、都会发送事件通知 `images/` 前缀。

b. 确认已向目标 SNS 主题发送通知。

例如，如果您的目标主题托管在 AWS 简单通知服务（ SNS ）上，则可以将此服务配置为在发送通知时向您发送电子邮件。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

如果在目标主题收到通知，则表示您已成功为 StorageGRID 通知配置源存储分段。

相关信息

"了解存储分段通知"

"使用S3 REST API"

"创建平台服务端点"

使用搜索集成服务

搜索集成服务是三种 StorageGRID 平台服务之一。您可以启用此服务，以便在创建，删除对象或更新其元数据或标记时将对象元数据发送到目标搜索索引。

您可以使用租户管理器将自定义 StorageGRID 配置 XML 应用于存储分段来配置搜索集成。

> 由于搜索集成服务会将对象元数据发送到目标，因此其配置 XML 称为 *metadata notification configuration xml* 。此配置 XML 与用于启用事件通知的 *notification* 配置 *xml* 不同。

请参见 "有关实施 S3 客户端应用程序的说明" 有关以下自定义 StorageGRID S3 REST API 操作的详细信息：

- 删除存储分段元数据通知配置
- 获取存储分段元数据通知配置
- PUT 存储分段元数据通知配置

相关信息

"用于搜索集成的配置 XML"

"元数据通知中包含的对象元数据"

"由搜索集成服务生成的 JSON"

"配置搜索集成服务"

"使用S3 REST API"

用于搜索集成的配置 **XML**

搜索集成服务使用中包含的一组规则进行配置 `<MetadataNotificationConfiguration>` 和 `</MetadataNotificationConfiguration>` 标记。每个规则都指定规则适用场景 所对应的对象以及 StorageGRID 应将这些对象的元数据发送到的目标。

可以按对象名称的前缀筛选对象。例如、您可以发送具有前缀的对象的元数据 `images` 一个目标、并为具有前缀的对象提供元数据 `videos` 另一个。前缀重叠的配置无效、在提交时将被拒绝。例如、一种配置、其中包含一个前缀为的对象规则 `test` 和第二个规则、用于具有前缀的对象 `test2` 不允许。

必须使用为搜索集成服务创建的 StorageGRID 端点的 URN 指定目标。这些端点是指 Elasticsearch 集群上定义的索引和类型。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

下表介绍了元数据通知配置 XML 中的元素。

Name	Description	Required
MetadataNotificationConfiguration	用于指定元数据通知的对象和目标的规则的容器标记。 包含一个或多个规则元素。	是的。
规则	用于标识应将其元数据添加到指定索引中的对象的规则的容器标记。 拒绝前缀重叠的规则。 包含在 MetadataNotificationConfiguration 元素中。	是的。
ID	规则的唯一标识符。 包含在 Rule 元素中。	否
Status	状态可以是 " 已启用 " 或 " 已禁用 " 。不会对已禁用的规则执行任何操作。 包含在 Rule 元素中。	是的。

Name	Description	Required
前缀	与前缀匹配的对象受此规则的影响，其元数据将发送到指定目标。 要匹配所有对象，请指定一个空前缀。 包含在 Rule 元素中。	是的。
目标	规则目标的容器标记。 包含在 Rule 元素中。	是的。
URN	发送对象元数据的目标的 urn 。必须是具有以下属性的 StorageGRID 端点的 URN： • `es` 必须是第三个元素。 • URN必须以存储元数据的索引和类型结尾、格式为 `domain-name/myindex/mytype`。 端点使用租户管理器或租户管理 API 进行配置。它们的形式如下： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 必须在提交配置 XML 之前配置端点，否则配置将失败并显示 404 错误。 urn 包含在目标元素中。	是的。

使用示例元数据通知配置 XML 了解如何构建自己的 XML 。

用于适用场景 所有对象的元数据通知配置

在此示例中，所有对象的对象元数据都将发送到同一目标。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

具有两个规则的元数据通知配置

在此示例中、是指与前缀匹配的对象的对象元数据 `/images` 发送到一个目标、而与前缀匹配的对象的对象元数据则发送到一个目标 `/videos` 发送到另一个目标。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

相关信息

"使用S3 REST API"

"元数据通知中包含的对象元数据"

"由搜索集成服务生成的 JSON"

"配置搜索集成服务"

每当创建，删除对象或更新其元数据或标记时，搜索集成服务都会将对象元数据发送到目标搜索索引。

开始之前

- StorageGRID 管理员已为租户帐户启用平台服务。
- 您已创建要为其内容编制索引的S3存储分段。
- 要用作搜索集成服务目标的端点已存在、并且您具有其URN。
- 您属于具有的用户组 "管理所有分段或root访问权限"。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

为源存储分段配置搜索集成服务后，创建对象或更新对象的元数据或标记会触发要发送到目标端点的对象元数据。如果为已包含对象的存储分段启用搜索集成服务、则不会自动为现有对象发送元数据通知。您必须更新这些现有对象，以确保其元数据已添加到目标搜索索引中。

步骤

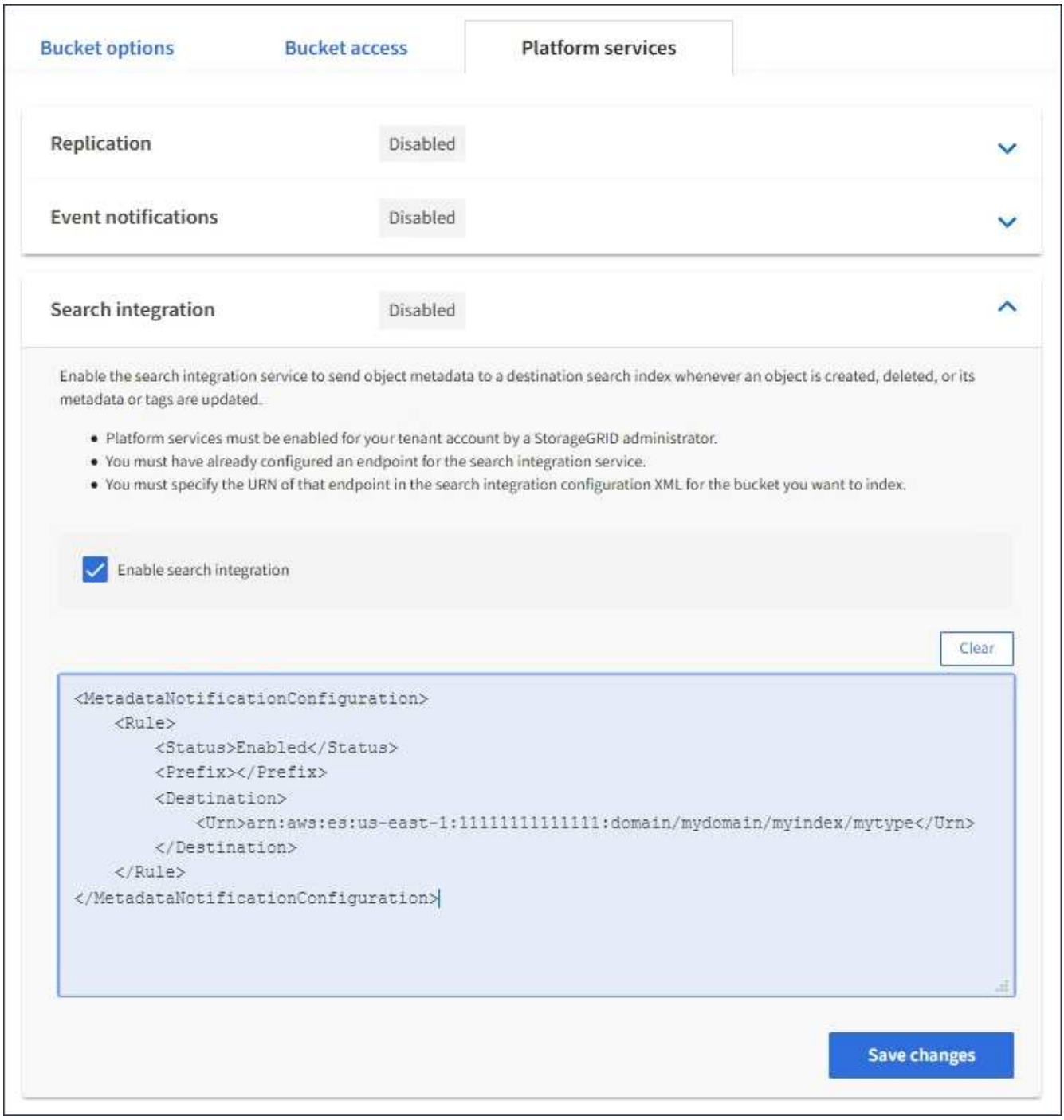
1. 使用文本编辑器创建启用搜索集成所需的元数据通知 XML 。
   - 请参见有关用于搜索集成的配置 XML 的信息。
   - 配置 XML 时，请使用搜索集成端点的 URN 作为目标。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 搜索集成 *
5. 选中*启用搜索集成*复选框。
6. 将元数据通知配置粘贴到文本框中，然后选择 * 保存更改 * 。



StorageGRID 管理员必须使用网格管理器或管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证是否已正确配置搜索集成服务：
   a. 向源存储分段添加一个对象，以满足配置 XML 中指定的元数据通知触发要求。

      在前面显示的示例中，添加到存储分段的所有对象都会触发元数据通知。

   b. 确认包含对象元数据和标记的 JSON 文档已添加到端点中指定的搜索索引中。

完成后

根据需要，您可以使用以下任一方法禁用存储分段的搜索集成：

- 选择*storage (S3)*>*Bucbes*并清除*Enable search integration*复选框。
- 如果您直接使用 S3 API ，请使用删除分段元数据通知请求。请参见有关实施 S3 客户端应用程序的说明。

相关信息

"了解搜索集成服务"

"用于搜索集成的配置 XML"

"使用S3 REST API"

"创建平台服务端点"

由搜索集成服务生成的 **JSON**

为存储分段启用搜索集成服务后，每次添加，更新或删除对象元数据或标记时，系统都会生成一个 JSON 文档并将其发送到目标端点。

此示例显示了使用密钥的对象时可能生成的JSON示例 `SGWS/Tagging.txt` 在名为的存储分段中创建 `test`。。 `test` 存储分段未进行版本控制、因此 `versionId` 标记为空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

元数据通知中包含的对象元数据

下表列出了启用搜索集成后发送到目标端点的 JSON 文档中包含的所有字段。

文档名称包括存储分段名称，对象名称和版本 ID （如果存在）。

Type	项目名称和问题描述
存储分段和对象信息	`bucket`：存储分段的名称
`key`：对象密钥名称	`versionID`：对象版本、用于受版本控制的分段中的对象
`region`：例如、Bucket区域 `us-east-1`	系统元数据
`size`：HTTP客户端可见的对象大小(以字节为单位)	`md5`：对象哈希
用户元数据	`metadata`：对象的所有用户元数据、作为键值对 `key:value`
Tags	`tags`：为对象定义的所有对象标记、作为键值对 `key:value`

对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后、无法在索引中编辑文档的域类型。