使用租户帐户
StorageGRID 11.5

NetApp
April 11, 2024

目录

使用租户帐户

了解如何使用StorageGRID 租户帐户。

- "使用租户管理器"
- "管理租户用户的系统访问"
- "管理S3租户帐户"
- "管理S3平台服务"

使用租户管理器

租户管理器允许您管理 StorageGRID 租户帐户的所有方面。

您可以使用租户管理器监控租户帐户的存储使用情况，并通过身份联合或创建本地组和用户来管理用户。对于 S3 租户帐户，您还可以管理 S3 密钥，管理 S3 存储分段以及配置平台服务。

使用**StorageGRID** 租户帐户

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。

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。

也可以使用租户帐户按不同的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。请参见有关实施 S3 客户端应用程序的说明。

- * 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。

创建租户帐户

租户帐户由 StorageGRID 网格管理员使用网格管理器创建。创建租户帐户时，网格管理员会指定以下信息：

- 租户的显示名称（租户的帐户 ID 会自动分配，不能更改）。
- 租户帐户是使用 S3 还是 Swift 。
- 对于 S3 租户帐户：是否允许租户帐户使用平台服务。如果允许使用平台服务，则必须对网格进行配置，以支持使用这些服务。
- （可选）租户帐户的存储配额—租户对象可用的最大 GB ， TB 或 PB 数。租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。
- 如果为 StorageGRID 系统启用了身份联合，则哪个联合组具有 " 根访问 " 权限来配置租户帐户。

- 如果 StorageGRID 系统未使用单点登录（ SSO ），则表示租户帐户是使用自己的身份源还是共享网格的身份源，以及租户的本地 root 用户的初始密码。

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

创建 S3 租户帐户后，您可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享）或创建本地组和用户
- 管理 S3 访问密钥
- 创建和管理 S3 存储分段，包括合规存储分段
- 使用平台服务（如果已启用）
- 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，但您必须具有 S3 访问密钥，并使用 S3 REST API 载入和管理对象。

配置**Swift**租户

创建 Swift 租户帐户后，具有 root 访问权限的用户可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享），并创建本地组和用户
- 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， " 根访问 " 权限不允许用户向 Swift REST API 进行身份验证以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。

相关信息

"管理 StorageGRID"

"使用 S3"

"使用 Swift"

Web 浏览器要求

您必须使用受支持的 Web 浏览器。

Web 浏览器	支持的最低版本
Google Chrome	87
Microsoft Edge	87

Web 浏览器	支持的最低版本
Mozilla Firefox	84.

您应将浏览器窗口设置为建议的宽度。

浏览器宽度	像素
最小值	1024
最佳	1280

登录到租户管理器

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

您需要的内容

- 您必须拥有登录凭据。
- 您必须具有网格管理员提供的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 始终包含用于访问管理节点的完全限定域名（ FQDN ）或 IP 地址，也可以包括端口号， 20 位租户帐户 ID 或这两者。

- 如果 URL 不包含租户的 20 位帐户 ID ，则必须具有此帐户 ID 。
- 您必须使用受支持的Web浏览器。
- 必须在 Web 浏览器中启用 Cookie 。
- 您必须具有特定的访问权限。

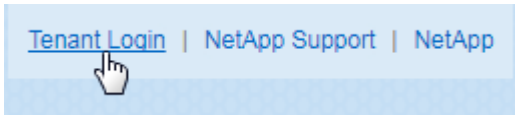
步骤

1. 启动受支持的 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 。

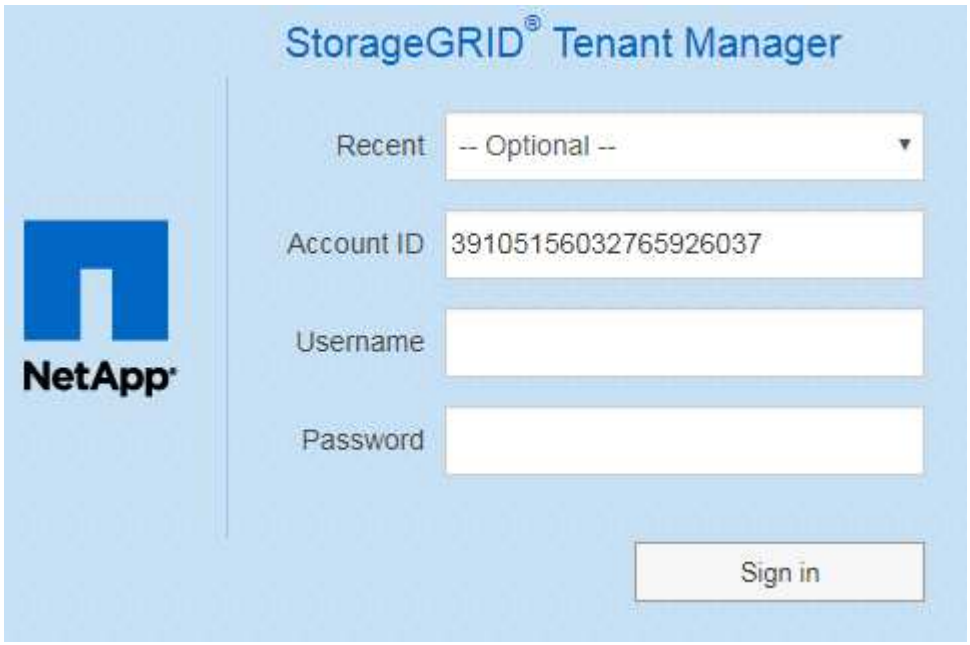
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。
4. 登录到租户管理器。

   您看到的登录屏幕取决于您输入的 URL 以及您的组织是否使用单点登录（ SSO ）。您将看到以下屏幕之一：

   - 网格管理器登录页面。单击右上角的 * 租户登录 * 链接。

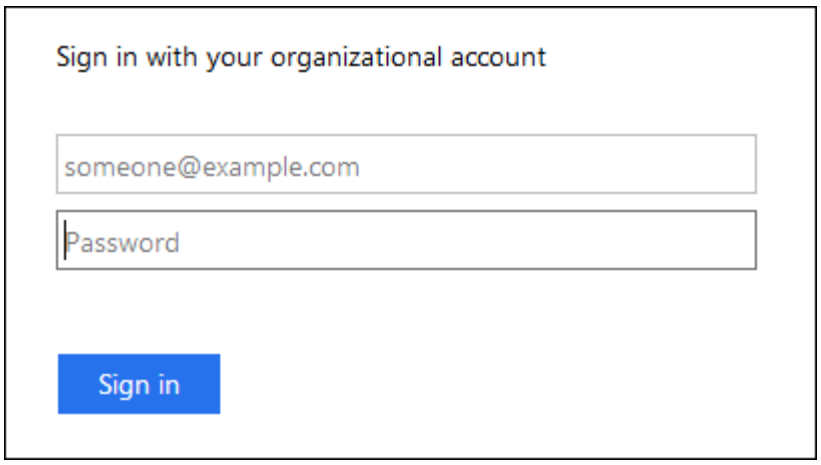
   - 租户管理器登录页面。* 帐户 ID* 字段可能已完成，如下所示。

     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. 单击 * 登录 * 。

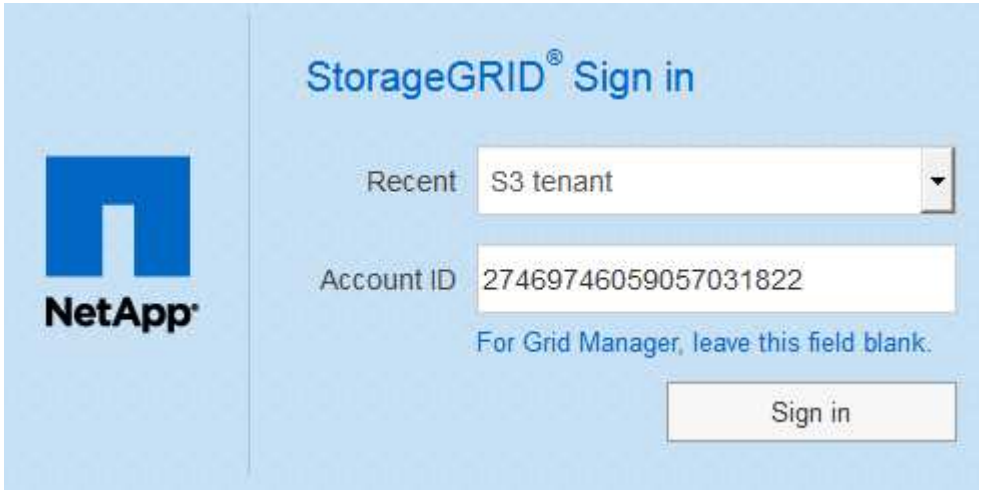
     此时将显示租户管理器信息板。

   - 如果在网格上启用了 SSO ，则为您所在组织的 SSO 页面。例如：



输入标准 SSO 凭据，然后单击 * 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. 单击 * 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。

5. 如果您从其他人收到初始密码，请更改密码以保护您的帐户。选择 * 。 username_* > * 更改密码 * 。

> 如果为 StorageGRID 系统启用了 SSO ，则无法从租户管理器更改密码。

相关信息

"管理 StorageGRID"

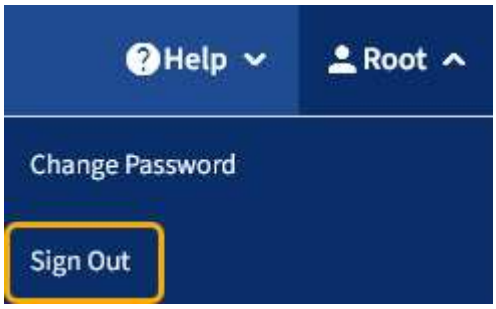
"Web 浏览器要求"

注销租户管理器

使用租户管理器后，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 * 注销 * 。

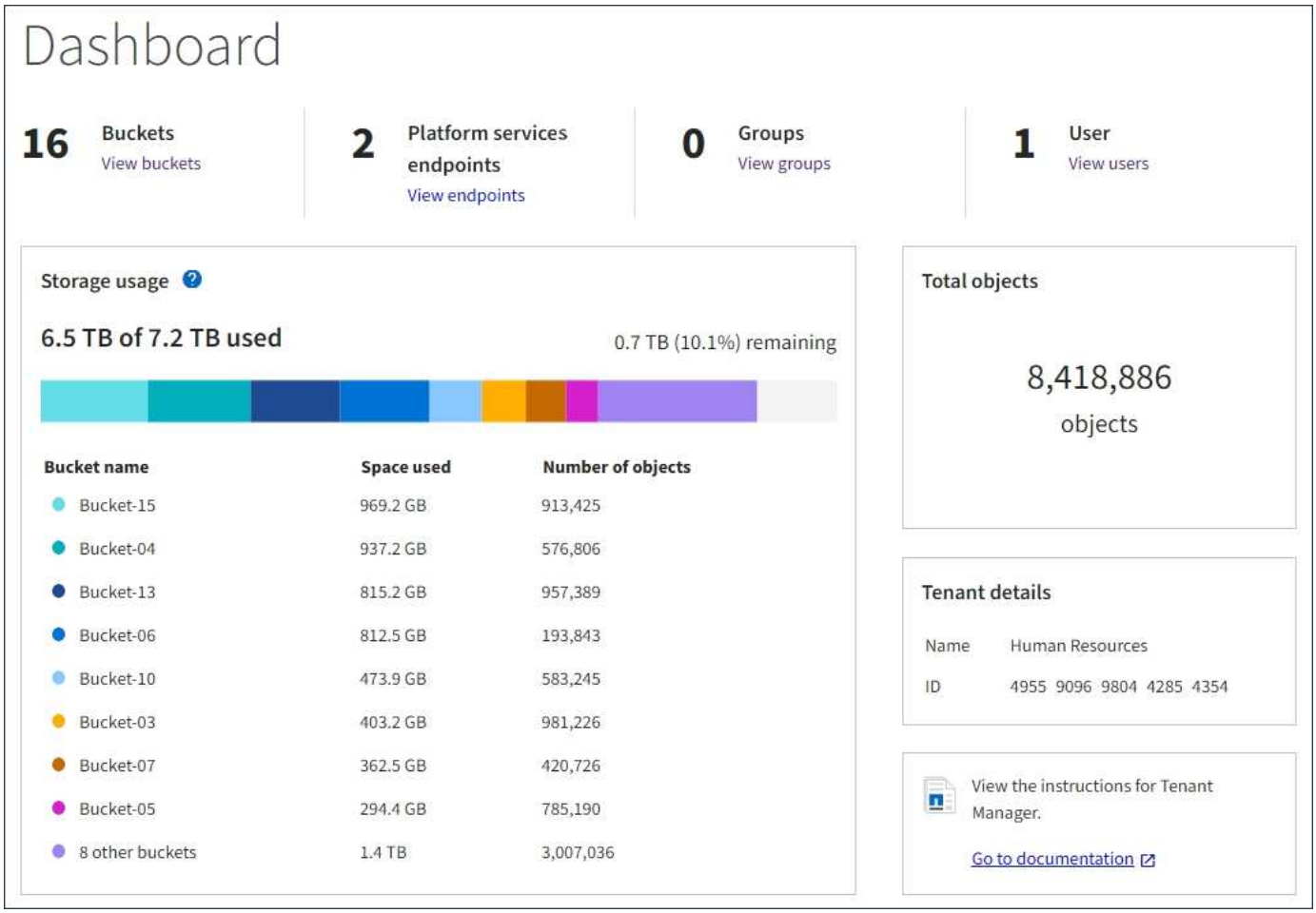
选项	Description
SSO 未使用	您已从管理节点注销。此时将显示租户管理器登录页面。 • 注意： * 如果您已登录到多个管理节点，则必须从每个节点注销。
已启用 SSO	您已从正在访问的所有管理节点中注销。此时将显示 StorageGRID 登录页面。您刚刚访问的租户帐户的名称将在 * 近期帐户 * 下拉列表中列为默认名称，并显示租户的 * 帐户 ID* 。 *注意：*如果启用了SSO、并且您还登录到网格管理器、则还必须注销网格管理器才能注销SSO。

了解租户管理器信息板

租户管理器信息板概述了租户帐户的配置以及租户分段（ S3 ）或容器（ Swift ）中的对象所使用的空间量。如果租户有配额，信息板将显示配额的已用量和剩余量。如果存在与租户帐户相关的任何错误，则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。

上传对象后，信息板类似于以下示例：



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，则会显示入门准则，而不是对象总数。

- 租户帐户名称和ID。
- 指向StorageGRID 文档的链接。

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。

配额利用率基于内部估计值，在某些情况下可能会超出此值。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，直到重新计算配额利用率为止。配额利用率计算可能需要 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。

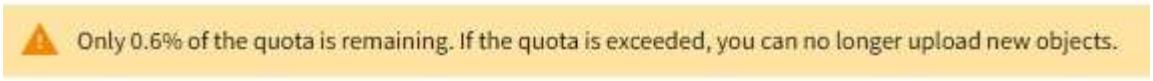
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

  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。

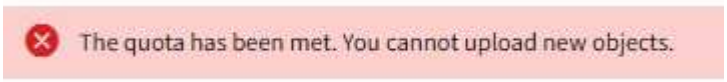
配额使用情况警报

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。有关详细信息，请参见 StorageGRID 监控和故障排除说明中的警报参考。



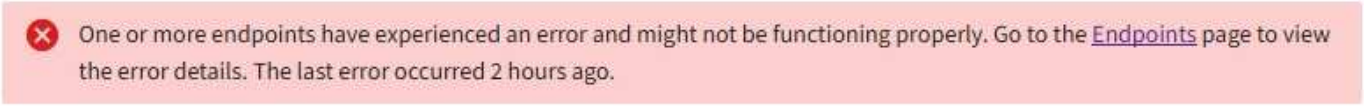
如果超过配额，则无法上传新对象。



要查看其他详细信息以及管理警报规则和通知，请参见有关监控 StorageGRID 和对其进行故障排除的说明。

端点错误

如果您已使用网格管理器配置一个或多个端点以用于平台服务，则如果在过去七天内发生任何端点错误，则租户管理器信息板将显示警报。



要查看有关端点错误的详细信息，请选择端点以显示端点页面。

相关信息

"解决平台服务端点错误"

"监控和放大；故障排除"

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。

要访问租户管理 API 的 Swagger 文档，请执行以下操作：

步骤

1. 登录到租户管理器。
2. 从租户管理器标题中选择*帮助*>* 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。
- * 身份验证 * —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。请参见管理StorageGRID 的说明中的"如果启用了单点登录、请参见`对API进行身份验证`"。

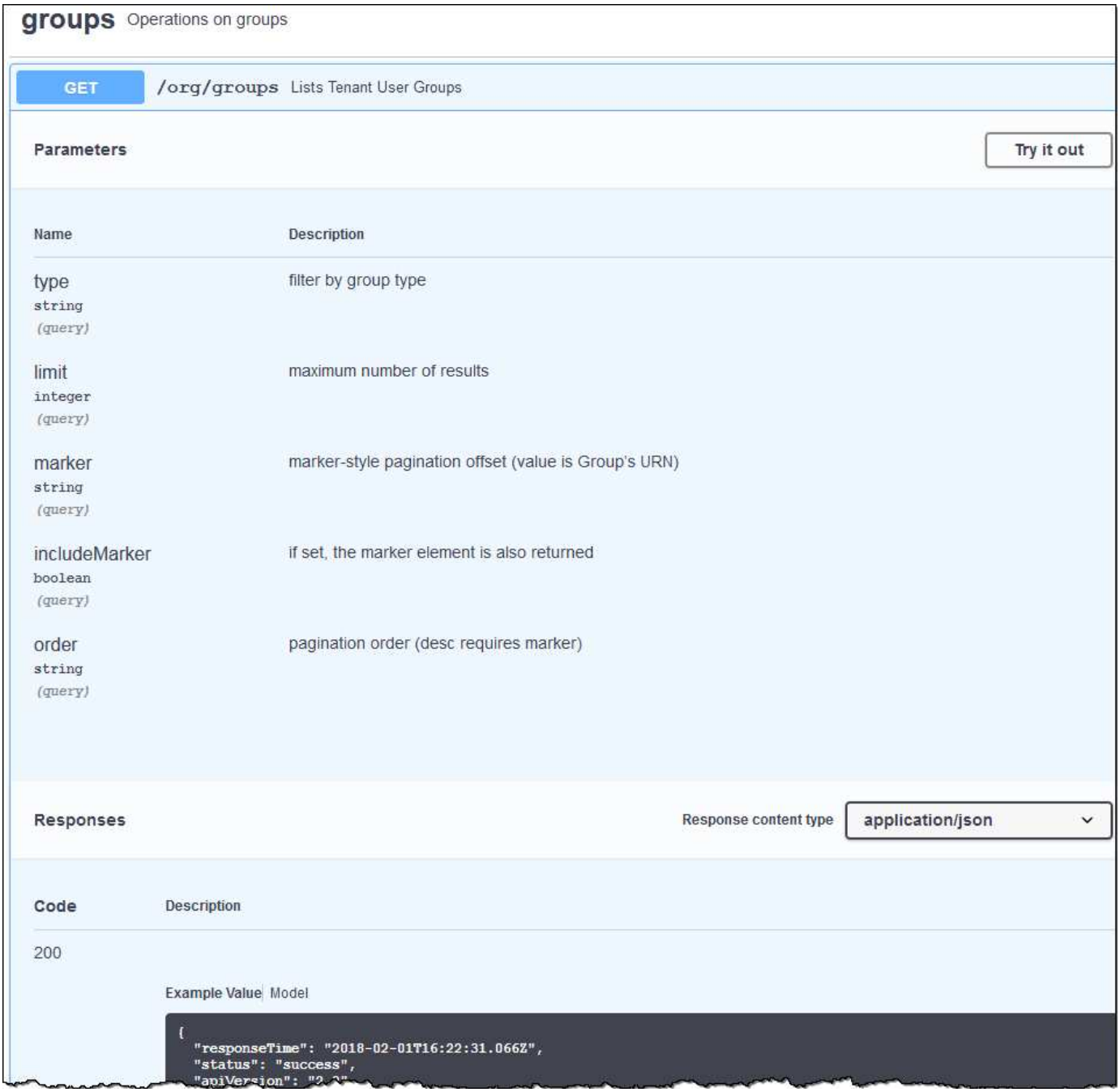
- **config** —与租户管理 API 的产品版本和版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 容器 * —对 S3 存储分段或 Swift 容器执行的操作如下：

协议	权限允许
S3	• 创建合规和不合规的存储分段 • 修改原有合规性设置 • 为对对象执行的操作设置一致性控制 • 创建、更新和删除存储分段的CORS配置 • 启用和禁用对象的上次访问时间更新 • 管理平台服务的配置设置、包括CloudMirror复制、通知和搜索集成(元数据通知) • 正在删除空存储分段
Swift	设置用于容器的一致性级别

- "*deactived-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。
- * 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。
- **identity-source** —用于配置外部身份源以及手动同步联合组和用户信息的操作。
- * 区域 * - 用于确定已为 StorageGRID 系统配置哪些区域的操作。
- * S3 * —用于管理租户用户 S3 访问密钥的操作。
- * s3-object-lock*—用于确定如何为StorageGRID 系统配置全局S3对象锁定(合规性)的操作。
- * 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。



发出**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. 单击HTTP操作可查看请求详细信息。
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、您可以单击*型号*来了解每个字段的要求。
4. 单击 * 试用 * 。

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

相关信息

"防止跨站点请求伪造(CSRF)"

"管理 StorageGRID"

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
```

如果对旧版本进行了 * 不兼容 _* 的更改，则租户管理 API 的主要版本将发生递增。如果对 * 与旧版本兼容 _* 进行了更改，则租户管理 API 的次要版本将发生递增。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
  ]
}
```

为请求指定**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。

有关其他示例和详细信息，请参见联机 API 文档。

> 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、

管理租户用户的系统访问

您可以通过从联合身份源导入组并分配管理权限来授予用户对租户帐户的访问权限。您还可以创建本地租户组和用户、除非对整个StorageGRID 系统实施单点登录(Single Sign-On、SSO)。

- "使用身份联合"
- "管理组"
- "管理本地用户"

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。

- "配置联合身份源"
- "强制与身份源同步"
- "正在禁用身份联合"

配置联合身份源

如果您希望在Active Directory、OpenLDAP或Oracle Directory Server等其他系统中管理租户组和用户、则可以配置身份联合。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有特定的访问权限。
- 您必须使用Active Directory、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、必须联系技术支持。
- 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 。

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。如果您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。

> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

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* Active Directory*、* OpenLDAP*或*其他*。

   如果选择* OpenLDAP*、请配置OpenLDAP服务器。请参见有关配置OpenLDAP服务器的准则。

   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。
   - * 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. 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服务器的服务器主机名或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`
   - * 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。

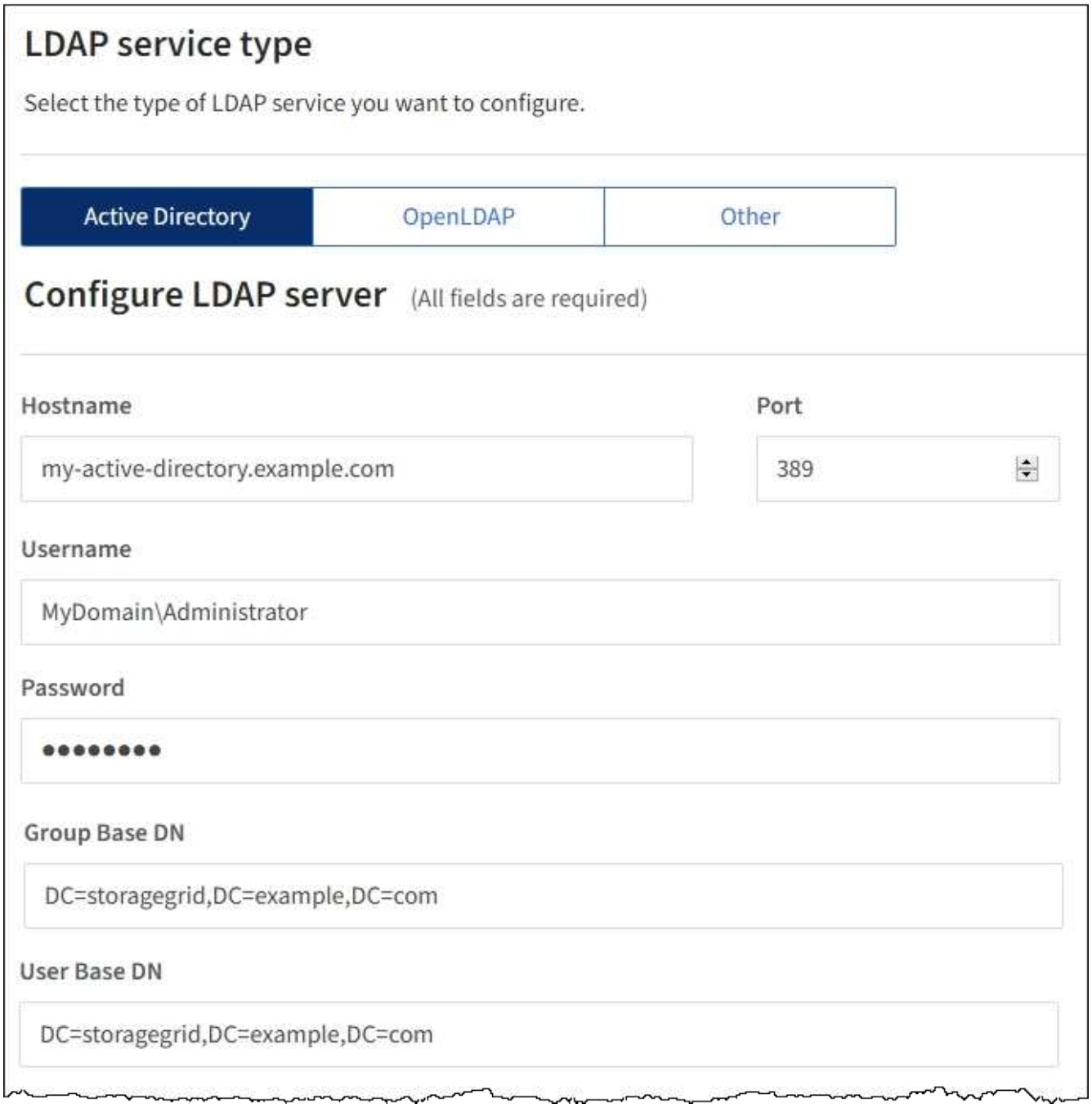
6. 在*传输层安全(TLS)*部分中、选择一个安全设置。
   - 使用**STARTTLS (**建议**)**：使用STARTTLS保护与LDAP服务器的通信安全。这是建议的选项。
   - * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。出于兼容性原因、支持此选项。
   - * 请勿使用 TLS* ： StorageGRID 系统与 LDAP 服务器之间的网络流量将不会受到保护。

     如果Active Directory服务器强制执行LDAP签名、则不支持此选项。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。
8. 选择*测试连接*以验证LDAP服务器的连接设置。

   如果连接有效、页面右上角将显示一条确认消息。
9. 如果连接有效、请选择*保存*。

   以下屏幕截图显示了使用Active Directory的LDAP服务器的示例配置值。



相关信息

"租户管理权限"

"配置 OpenLDAP 服务器的准则"

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。

memberOf 和 fint 覆盖

应启用成员和精简覆盖。有关详细信息、请参见《OpenLDAP管理员指南》中有关反向组成员资格维护的说明。

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OpenLDAP管理员指南中有关反向组成员资格维护的信息。

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有特定的访问权限。
- 必须启用已保存的身份源。

步骤

1. 选择 * 访问管理 * > * 身份联合 * 。

   此时将显示"Identity Federation"页面。*同步服务器*按钮位于页面右上角。

   如果未启用保存的身份源、则*同步服务器*按钮将不会处于活动状态。

2. 选择*同步服务器*。

   此时将显示一条确认消息、指示同步已成功启动。

相关信息

"租户管理权限"

正在禁用身份联合

如果为此租户配置了身份联合服务、则可以临时或永久禁用租户组和用户的身份联合。禁用身份联合后、StorageGRID 系统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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有特定的访问权限。

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租户帐户的访问权限、直到其会话到期为止、但在会话到期后、他们将无法登录。
- StorageGRID 系统与身份源之间不会进行同步。

步骤

1. 选择 * 访问管理 * > * 身份联合 * 。
2. 取消选中*启用身份联合*复选框。
3. 选择 * 保存 * 。

相关信息

"租户管理权限"

管理组

您可以为用户组分配权限，以控制租户用户可以执行的任务。您可以从身份源（例如 Active Directory 或 OpenLDAP ）导入联合组，也可以创建本地组。

> 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，但他们可以根据组权限访问 S3 和 Swift 资源。

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。由于缓存，更改可能需要长达 15

分钟才能生效。

权限	Description
根访问	提供对租户管理器和租户管理 API 的完全访问权限。 • 注： * 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	仅限 S3 租户。允许用户创建和删除自己的 S3 访问密钥。没有此权限的用户不会看到 * 存储（ S3 ） * > * 我的 S3 访问密钥 * 菜单选项。
管理所有分段	• 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。 没有此权限的用户不会看到 * 分段 * 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： * 您只能通过租户管理 API 为 Swift 组分配 " 管理所有分段 " 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	仅限 S3 租户。允许用户使用租户管理器或租户管理 API 创建或编辑端点，这些端点用作 StorageGRID 平台服务的目标。 没有此权限的用户不会看到 * 平台服务端点 * 菜单选项。

相关信息

"使用 S3"

"使用 Swift"

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选择 * 创建组 * 。
3. 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。

4. 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。
5. 选择 * 继续 * 。
6. 选择访问模式。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。
   - * 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。他们不能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。
7. 选择此组的组权限。

   请参见有关租户管理权限的信息。

8. 选择 * 继续 * 。
9. 选择组策略以确定此组的成员将拥有哪些 S3 访问权限。
   - * 无 S3 访问 * ： 默认值。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。您不能编辑此字符串。

- * 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。您不能编辑此字符串。
- * 自定义 * ： 组中的用户将获得您在文本框中指定的权限。有关组策略的详细信息，包括语言语法和示例，请参见实施 S3 客户端应用程序的说明。

10. 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。

    在此示例中，只允许组成员列出和访问指定存储分段中与其用户名（密钥前缀）匹配的文件夹。请注意，在确定其他组策略和存储分段策略的隐私时，应考虑这些文件夹的访问权限。

11. 根据要创建的是联合组还是本地组，选择显示的按钮：

    - 联合组： * 创建组 *
    - 本地组： * 继续 *

    如果要创建本地组，请在选择 * 继续 * 后显示步骤 4 （添加用户）。对于联合组，不会显示此步骤。

12. 选中要添加到组的每个用户对应的复选框，然后选择 * 创建组 * 。

    或者，您也可以在不添加用户的情况下保存组。您可以稍后将用户添加到组中，也可以在添加新用户时选择组。

13. 选择 * 完成 * 。

    您创建的组将显示在组列表中。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

"使用 S3"

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选择 * 创建组 * 。
3. 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。

4. 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。
5. 选择 * 继续 * 。

6. 选择访问模式。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。
   - * 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。他们不能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。
7. 设置组权限。
   - 如果用户需要登录到租户管理器或租户管理 API ，请选中 * 根访问 * 复选框。（默认）
   - 如果用户不需要访问租户管理器或租户管理 API ，请取消选中 * 根访问 * 复选框。例如，取消选中不需要访问租户的应用程序对应的复选框。然后，分配 * Swift 管理员 * 权限，以允许这些用户管理容器和对象。
8. 选择 * 继续 * 。
9. 如果用户需要能够使用 Swift REST API ，请选中 * Swift administrator* 复选框。

   Swift 用户必须具有 root 访问权限才能访问租户管理器。但是，" 根访问 " 权限不允许用户向 Swift REST API 进行身份验证以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。
10. 根据要创建的是联合组还是本地组，选择显示的按钮：
    - 联合组： * 创建组 *
    - 本地组： * 继续 *

      如果要创建本地组，请在选择 * 继续 * 后显示步骤 4 （添加用户）。对于联合组，不会显示此步骤。
11. 选中要添加到组的每个用户对应的复选框，然后选择 * 创建组 * 。

    或者，您也可以在不添加用户的情况下保存组。您可以稍后将用户添加到组中，也可以在创建新用户时选择组。
12. 选择 * 完成 * 。

    您创建的组将显示在组列表中。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

"使用 Swift"

查看和编辑组详细信息

查看组的详细信息时，您可以更改组的显示名称，权限，策略以及属于该组的用户。

您需要的内容

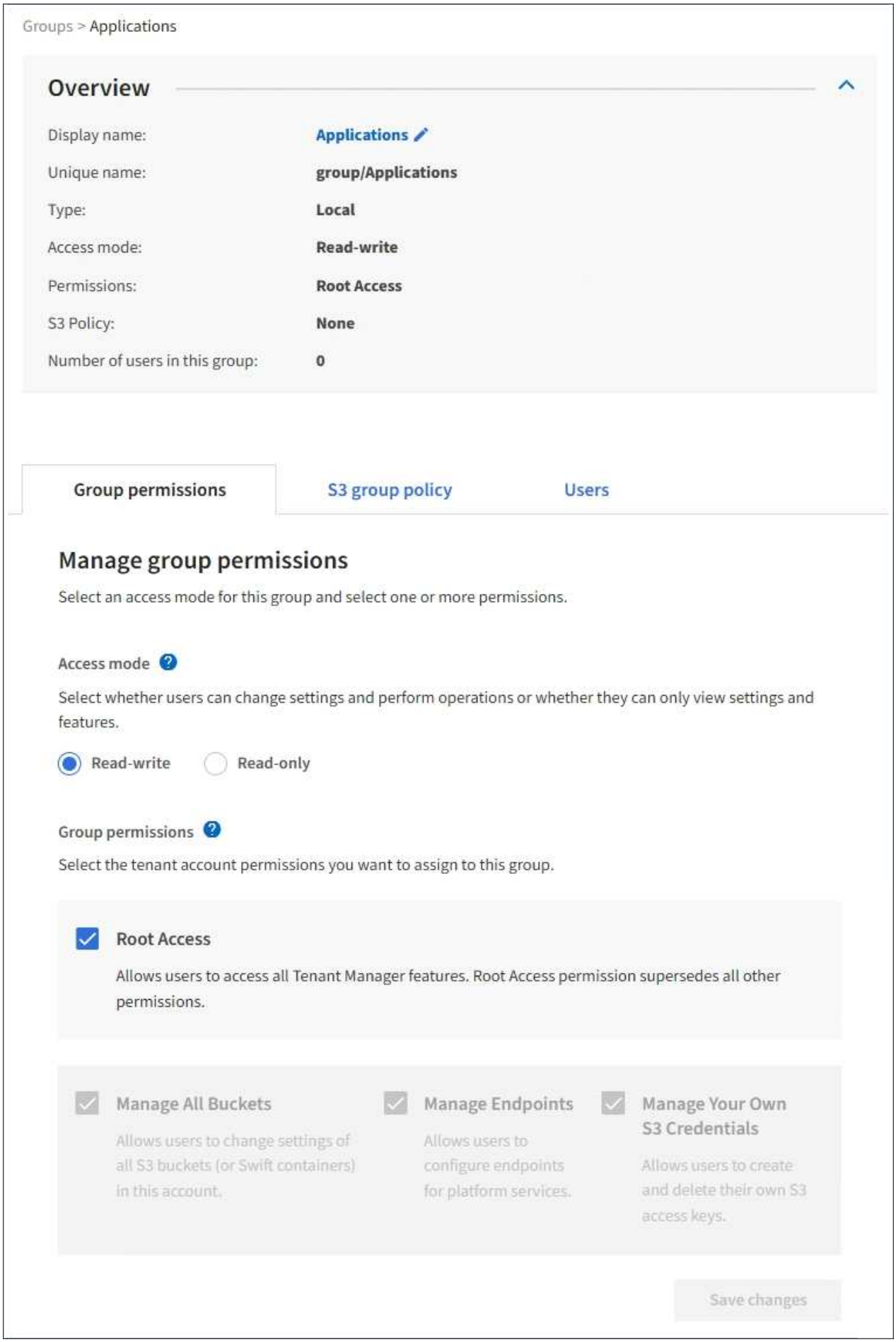
- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选择要查看或编辑其详细信息的组的名称。

   或者，您也可以选择 * 操作 * > * 查看组详细信息 * 。

   此时将显示组详细信息页面。以下示例显示了 S3 组详细信息页面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 根据需要更改组设置。

   要确保更改已保存，请在每个部分进行更改后选择 * 保存更改 * 。保存所做的更改后，页面右上角将显示一条确认消息。

   a. 也可以选择显示名称或编辑图标 更新显示名称。

      您不能更改组的唯一名称。您不能编辑联合组的显示名称。

   b. 也可以更新权限。

   c. 对于组策略，请为 S3 或 Swift 租户进行相应的更改。

      - 如果要编辑 S3 租户的组，也可以选择其他 S3 组策略。如果选择自定义 S3 策略，请根据需要更新 JSON 字符串。
      - 如果要编辑 Swift 租户的组，也可以选中或取消选中 * Swift 管理员 * 复选框。

        有关 Swift 管理员权限的详细信息，请参见有关为 Swift 租户创建组的说明。

   d. 也可以添加或删除用户。

4. 确认您已为更改的每个部分选择 * 保存更改 * 。

   由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"为S3租户创建组"

"为Swift租户创建组"

将用户添加到本地组

您可以根据需要将用户添加到本地组。

您需要的内容

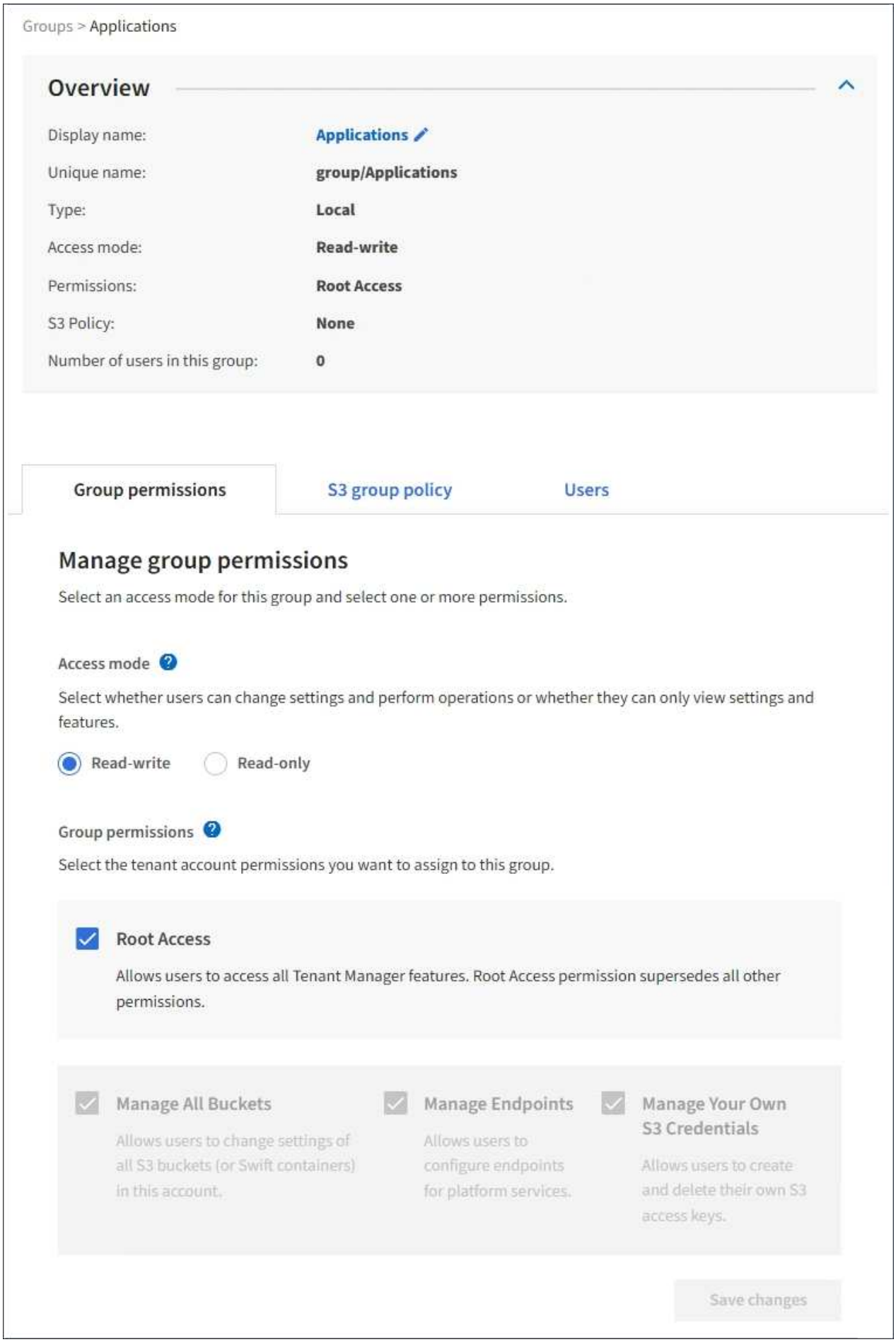
- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

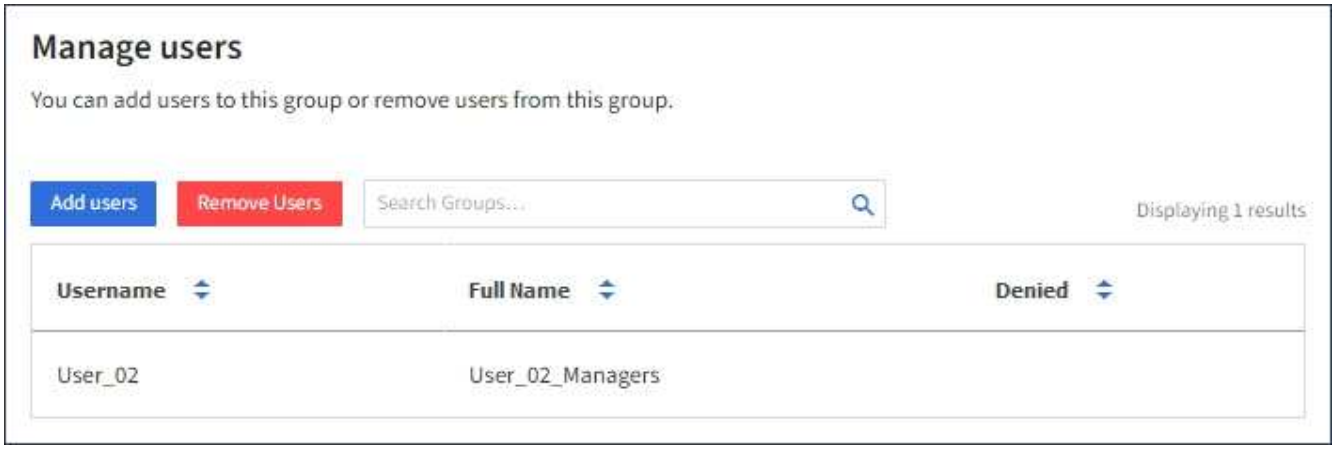
1. 选择 * 访问管理 * > * 组 * 。
2. 选择要将用户添加到的本地组的名称。

   或者，您也可以选择 * 操作 * > * 查看组详细信息 * 。

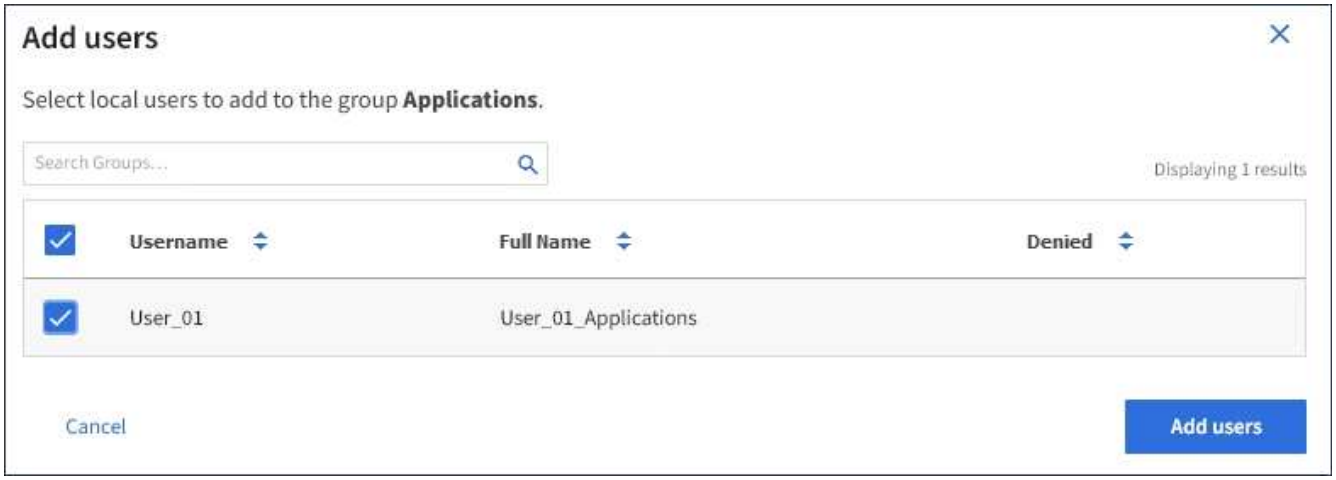
   此时将显示组详细信息页面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 选择*管理用户*、然后选择*添加用户*。



4. 选择要添加到组中的用户，然后选择 * 添加用户 * 。



页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

编辑组名称

您可以编辑组的显示名称。您不能编辑组的唯一名称。

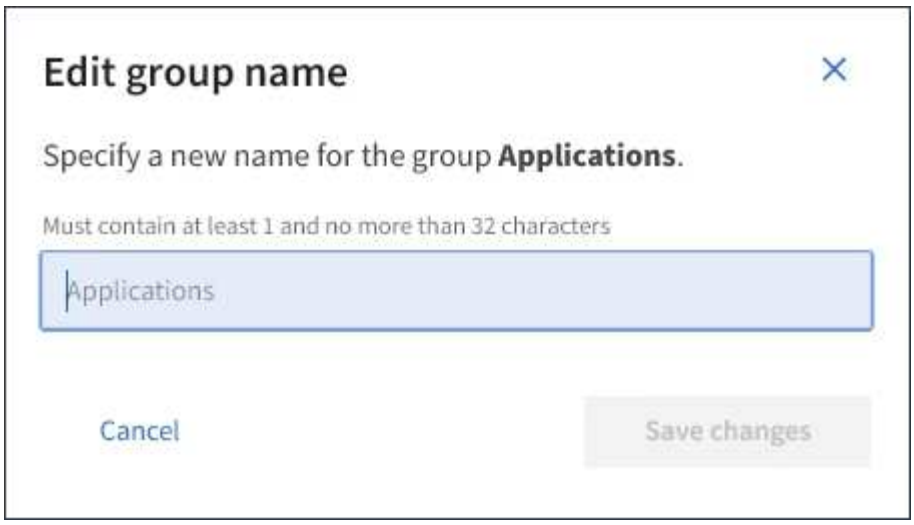
您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选中要编辑其显示名称的组对应的复选框。
3. 选择 * 操作 * > * 编辑组名称 * 。

   此时将显示编辑组名称对话框。



4. 如果要编辑本地组，请根据需要更新显示名称。

   您不能更改组的唯一名称。您不能编辑联合组的显示名称。

5. 选择 * 保存更改 * 。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

复制组

您可以通过复制现有组来更快地创建新组。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

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 * 复制组 * 。有关创建组的其他详细信息、请参见有关为S3租户或Swift租户创建组的说明。
4. 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。

5. 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。

6. 选择 * 继续 * 。
7. 根据需要修改此组的权限。
8. 选择 * 继续 * 。
9. 如果要为 S3 租户复制组，可以根据需要从 * 添加 S3 策略 * 单选按钮中选择其他策略。如果选择了自定义策略，请根据需要更新 JSON 字符串。
10. 选择 * 创建组 * 。

相关信息

"为S3租户创建组"

"为Swift租户创建组"

"租户管理权限"

删除组

您可以从系统中删除组。仅属于该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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选中要删除的组对应的复选框。
3. 选择 * 操作 * > * 删除组 * 。

此时将显示一条确认消息。

4. 选择 * 删除组 * 确认要删除确认消息中指示的组。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

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名为 "`root" 的预定义本地用户。` 虽然您可以添加和删除本地用户，但不能删除 root 用户。

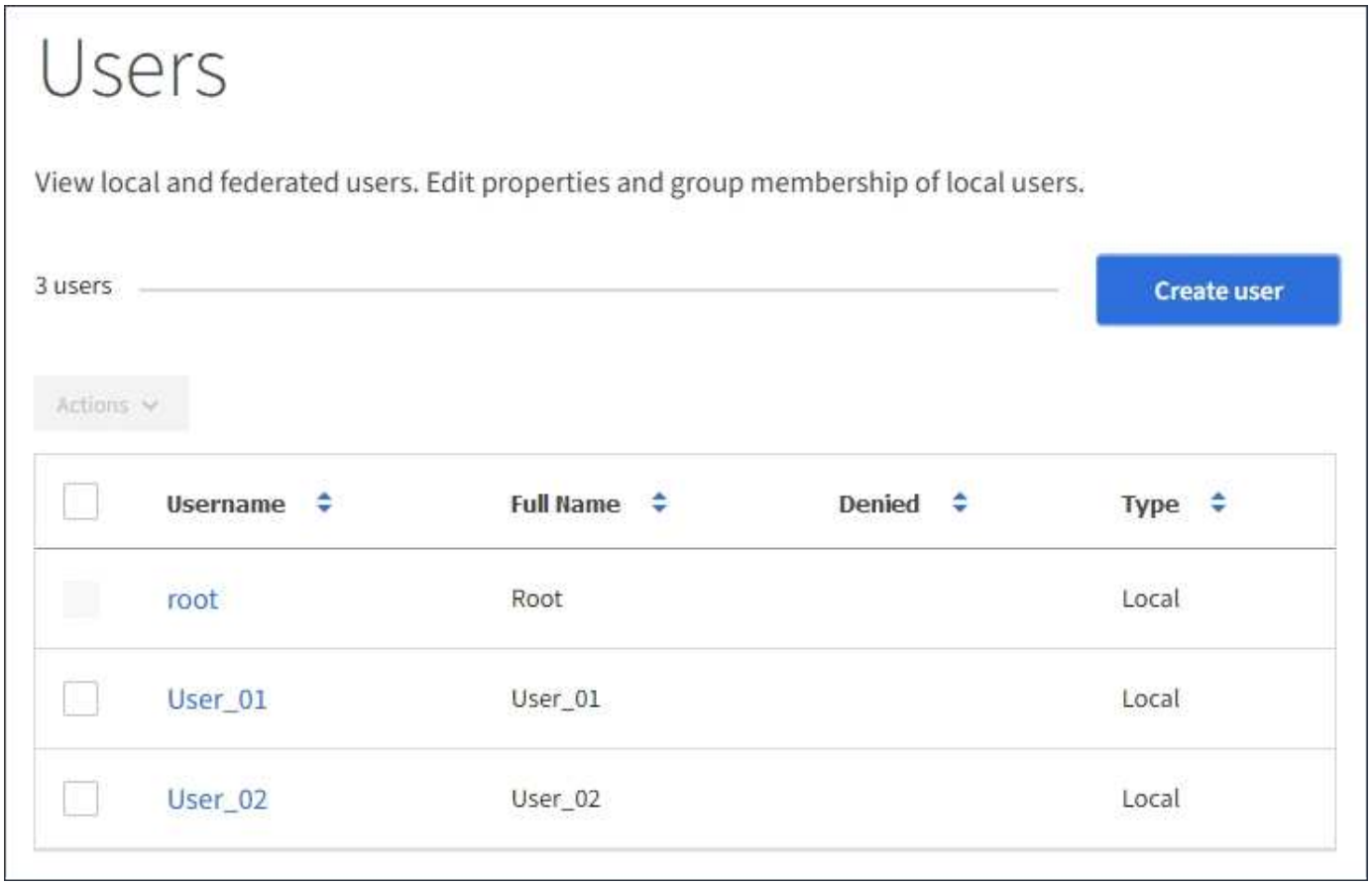
您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的读写用户组。

> 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 ，但他们可以根据组权限使用 S3 或 Swift 客户端应用程序访问租户的资源。

访问用户页面

选择 * 访问管理 * > * 用户 * 。



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 用户没有应用管理权限或 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 用户不具有管理权限或 Swift 容器访问权限。

步骤

1. 选择 * 创建用户 * 。
2. 填写以下字段。
   - * 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。
   - * 用户名 * ： 此用户用于登录的名称。用户名必须是唯一的，不能更改。
   - * 密码 * ： 用户登录时使用的密码。
   - * 确认密码 * ： 键入您在密码字段中键入的相同密码。
   - * 拒绝访问 * ： 如果选择 * 是 * ，则此用户无法登录到租户帐户，即使此用户可能仍属于一个或多个组。

     例如，您可以使用此功能暂时暂停用户的登录能力。
3. 选择 * 继续 * 。
4. 将用户分配给一个或多个本地组。

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。

5. 选择 * 创建用户 * 。

   由于缓存，更改可能需要长达 15 分钟才能生效。

编辑用户详细信息

编辑用户的详细信息时，您可以更改用户的全名和密码，将用户添加到不同的组并阻止用户访问租户。

步骤

1. 在用户列表中，选择要查看或编辑其详细信息的用户的名称。

   或者，您也可以选中用户的复选框，然后选择 * 操作 * > * 查看用户详细信息 * 。

2. 根据需要更改用户设置。
   a. 选择全名或编辑图标，根据需要更改用户的全名  在概述部分。

      您不能更改用户名。

   b. 在 * 密码 * 选项卡上，根据需要更改用户的密码。
   c. 在 * 访问 * 选项卡上，允许用户登录（选择 * 否 * ），或者根据需要阻止用户登录（选择 * 是 * ）。
   d. 在 * 组 * 选项卡上，根据需要将用户添加到组或从组中删除该用户。
   e. 根据需要为每个部分选择 * 保存更改 * 。

      由于缓存，更改可能需要长达 15 分钟才能生效。

复制本地用户

您可以复制本地用户以更快地创建新用户。

步骤

1. 在用户列表中，选择要复制的用户。
2. 选择 * 复制用户 * 。
3. 修改新用户的以下字段。
   - * 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。
   - * 用户名 * ： 此用户用于登录的名称。用户名必须是唯一的，不能更改。
   - * 密码 * ： 用户登录时使用的密码。
   - * 确认密码 * ： 键入您在密码字段中键入的相同密码。
   - * 拒绝访问 * ： 如果选择 * 是 * ，则此用户无法登录到租户帐户，即使此用户可能仍属于一个或多个组。

     例如，您可以使用此功能暂时暂停用户的登录能力。

4. 选择 * 继续 * 。

5. 选择一个或多个本地组。

   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。

6. 选择 * 创建用户 * 。

   由于缓存，更改可能需要长达 15 分钟才能生效。

正在删除本地用户

您可以永久删除不再需要访问 StorageGRID 租户帐户的本地用户。

使用租户管理器，您可以删除本地用户，但不能删除联合用户。您必须使用联合身份源删除联合用户。

步骤

1. 在用户列表中，选中要删除的本地用户对应的复选框。
2. 选择 * 操作 * > * 删除用户 * 。
3. 在确认对话框中，选择 * 删除用户 * 以确认要从系统中删除此用户。

   由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

管理S3租户帐户

您可以使用租户管理器管理S3访问密钥以及创建和管理S3存储分段。

- "管理 S3 访问密钥"
- "管理S3存储分段"

管理 S3 访问密钥

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。

关于此任务

S3 访问密钥可按如下方式进行管理：

- 具有 * 管理自己的 S3 凭据 * 权限的用户可以创建或删除自己的 S3 访问密钥。
- 具有 * 根访问 * 权限的用户可以管理 S3 根帐户和所有其他用户的访问密钥。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。要访问 S3 租户帐户中的分段和对象，您必须具有访问密钥。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有管理自己的 S3 凭据权限。

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。为安全起见，请勿创建超出您需要的密钥，并删除您未使用的密钥。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，则无需为密钥设置到期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。

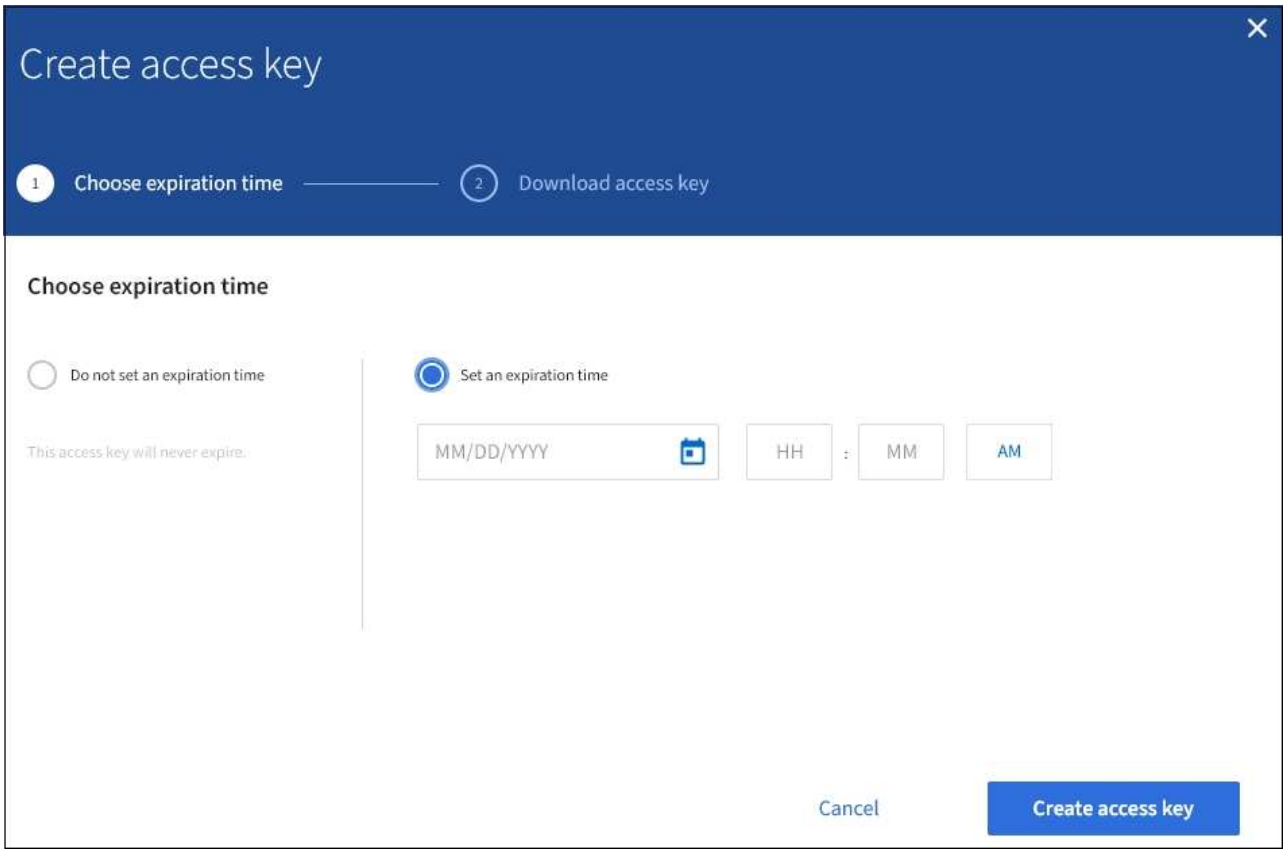
> 您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

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。

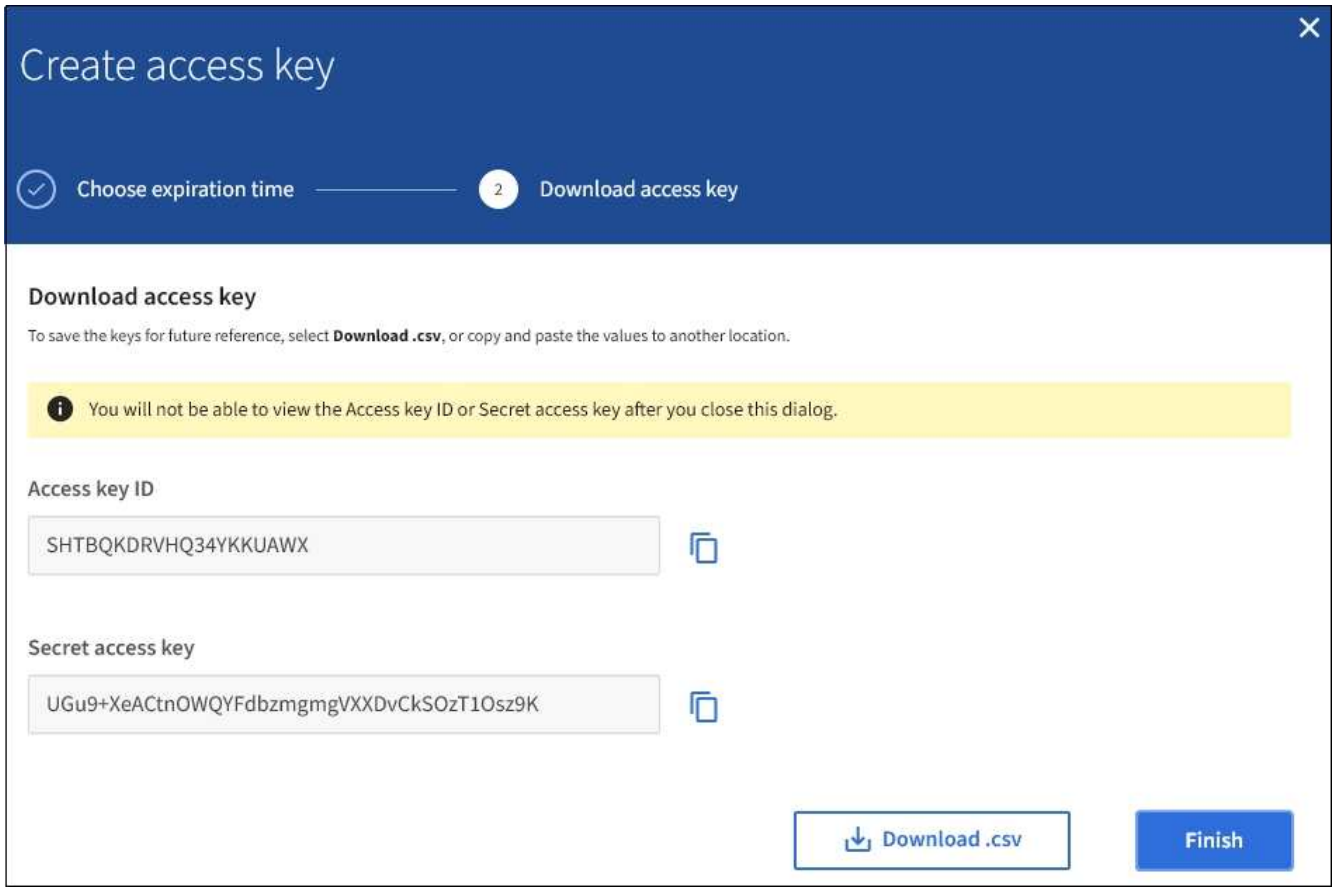


4. 选择 * 创建访问密钥 * 。

   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。

   在复制或下载此信息之前，请勿关闭此对话框。



6. 选择 * 完成 * 。

   新密钥将列在 " 我的访问密钥 " 页面上。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

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。您可以根据需要创建新密钥或删除不再使用的密钥。

您需要的内容

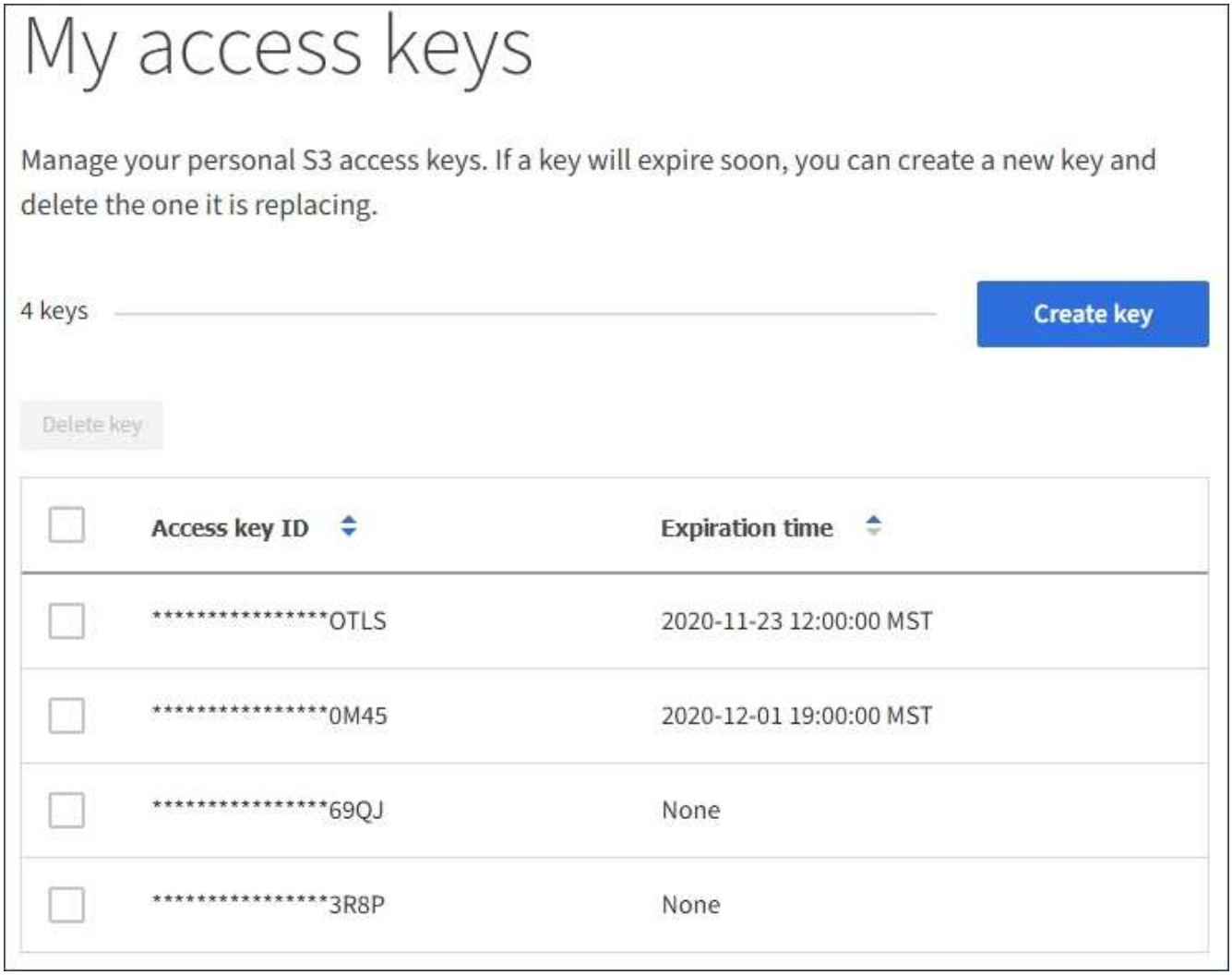
- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有管理自己的 S3 凭据权限。

> 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 * 。

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



2. 按 * 到期时间 * 或 * 访问密钥 ID* 对密钥进行排序。
3. 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

"创建您自己的S3访问密钥"

"删除您自己的S3访问密钥"

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有管理自己的 S3 凭据权限。

> 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。

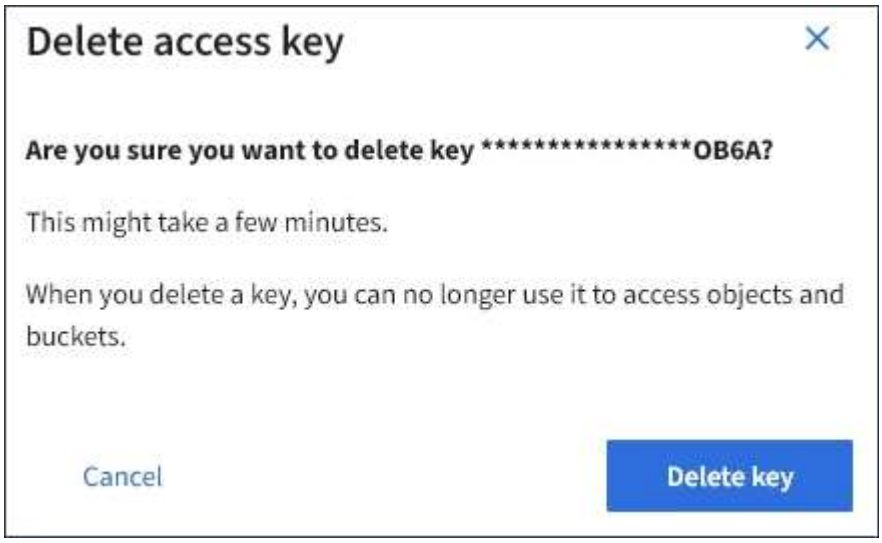
步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。

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

2. 选中要删除的每个访问密钥对应的复选框。
3. 选择 * 删除密钥 * 。

   此时将显示确认对话框。



4. 选择 * 删除密钥 * 。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有 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。为安全起见，请勿创建超出用户需求的密钥，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：

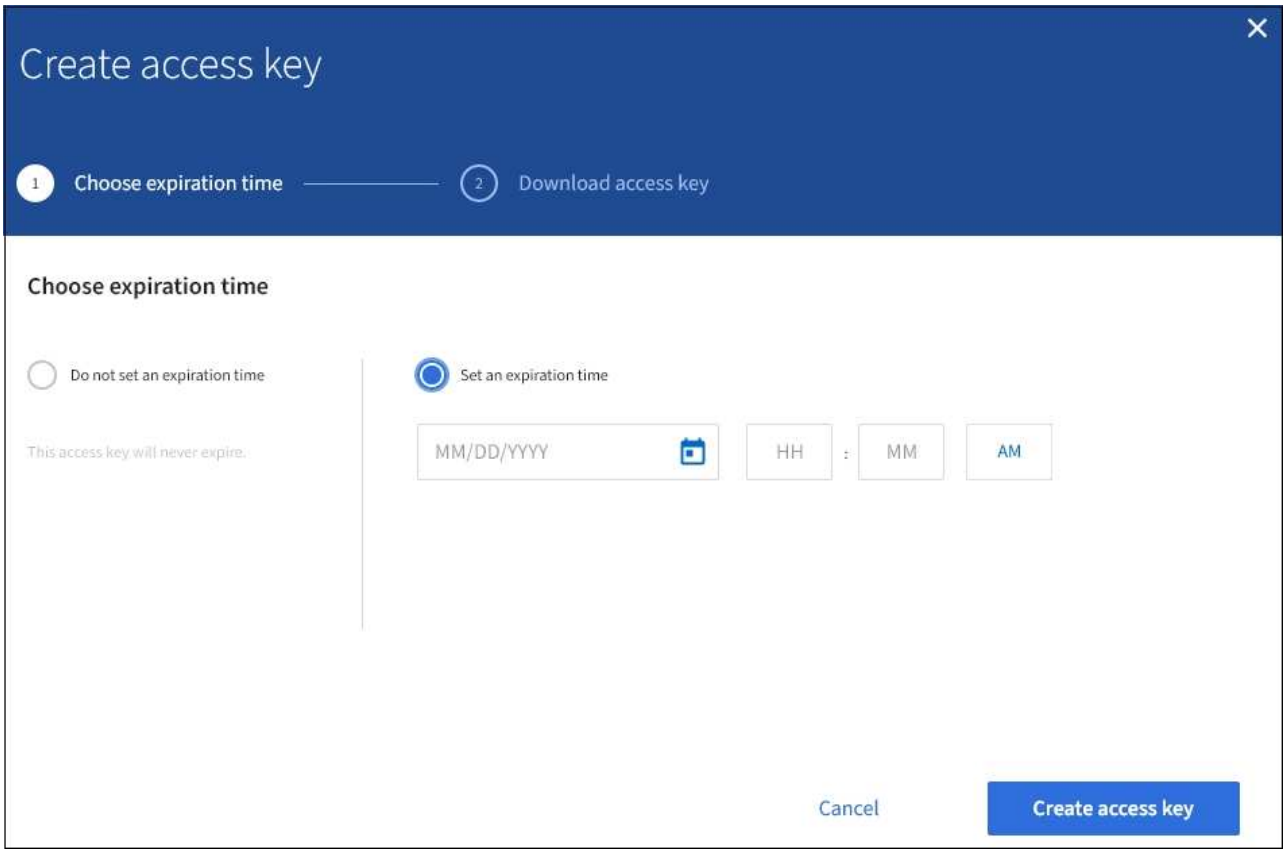
- 设置密钥的到期时间，以将用户的访问限制为特定时间段。如果访问密钥 ID 和机密访问密钥意外暴露，则设置较短的到期时间有助于降低风险。过期密钥将自动删除。
- 如果环境中的安全风险较低，并且您不需要定期创建新密钥，则无需为密钥设置到期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。

> 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 * 可创建未过期的密钥。（默认）
   - 选择 * 设置到期时间 * ，然后设置到期日期和时间。

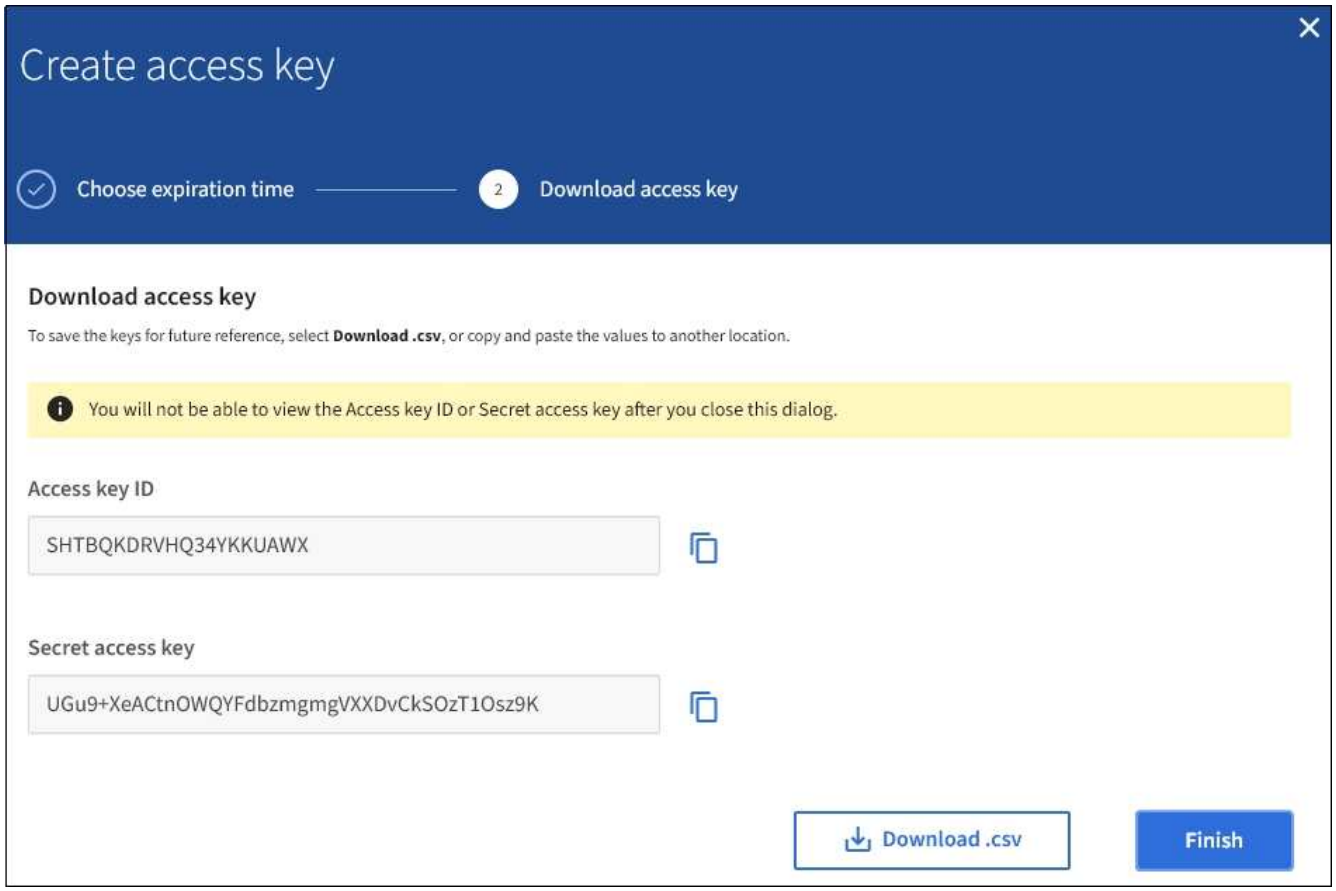


5. 选择 * 创建访问密钥 * 。

   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。

   在复制或下载此信息之前，请勿关闭此对话框。



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。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有 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

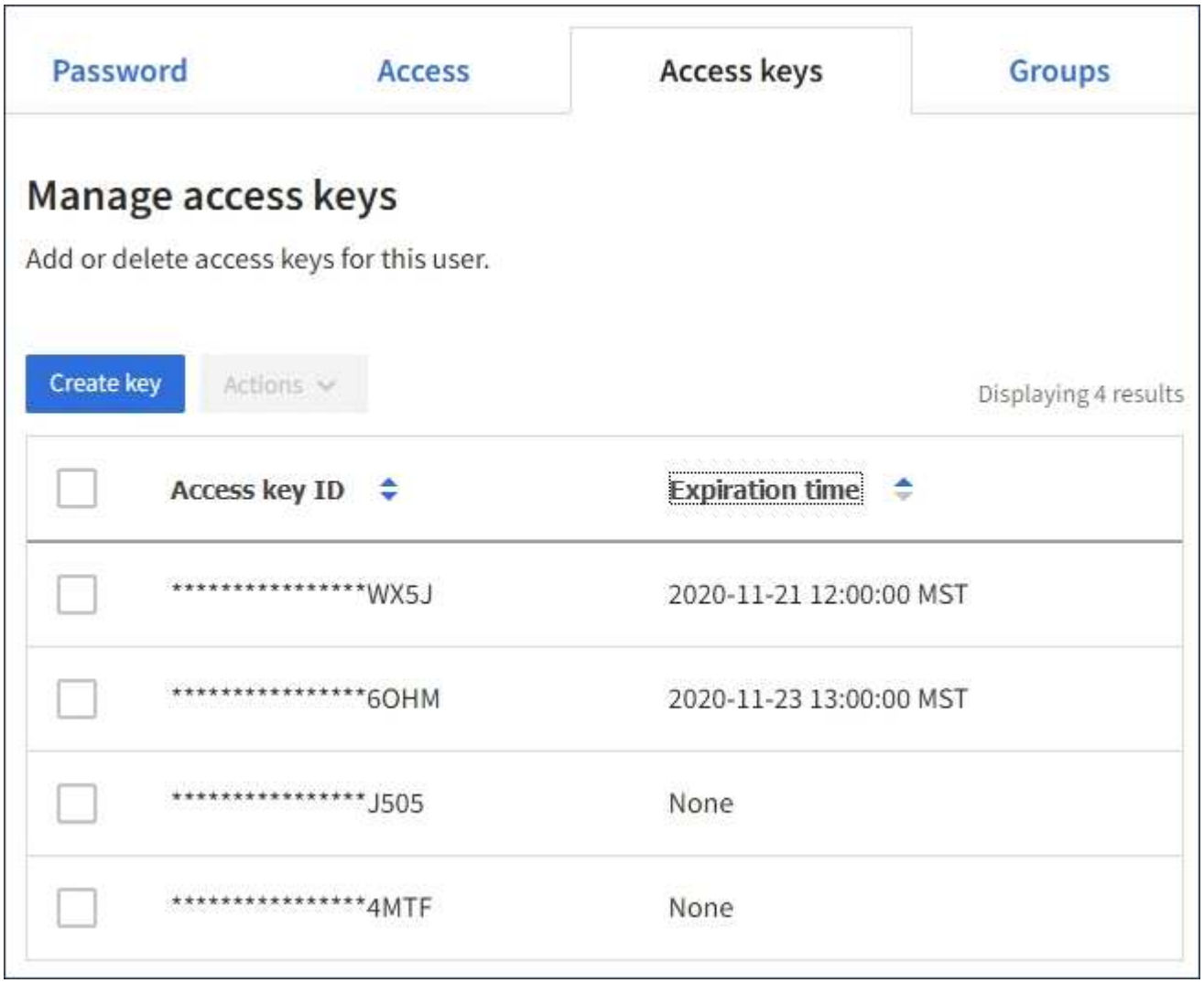
1. 选择 * 访问管理 * > * 用户 * 。

此时将显示 "Users" 页面，其中列出了现有用户。

2. 选择要查看其 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 * 。



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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有 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 * 。

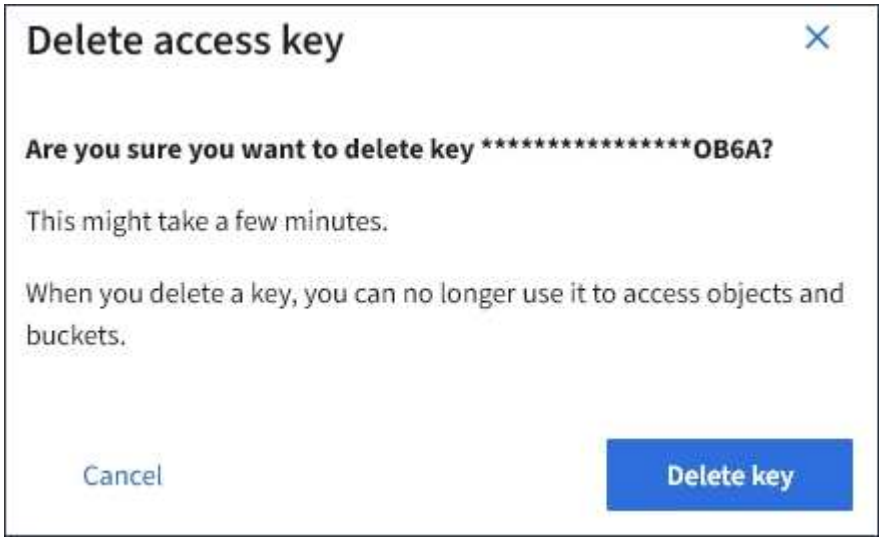
   此时将显示 "Users" 页面，其中列出了现有用户。

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 * 。

   此时将显示确认对话框。



5. 选择 * 删除密钥 * 。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

管理S3存储分段

如果您使用的是具有相应权限的S3租户、则可以创建、查看和删除S3存储分段、更新一致性级别设置、配置跨源资源共享(CORS)、启用和禁用上次访问时间更新设置以及管理S3平台服务。

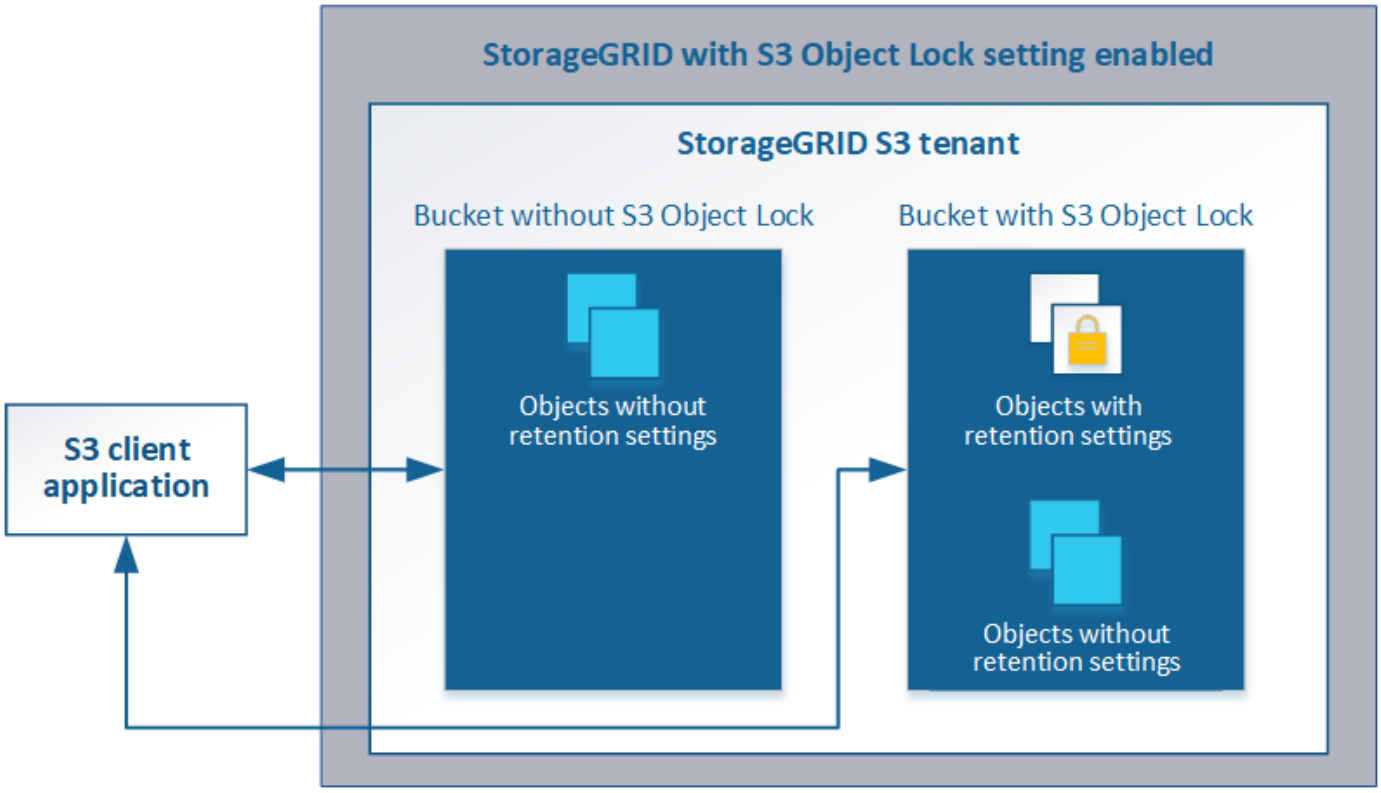
使用 S3 对象锁定

如果您的对象必须符合保留方面的法规要求，则可以使用 StorageGRID 中的 S3 对象锁定功能。

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。如果某个存储分段启用了 S3 对象锁定，则 S3 客户端应用程序可以选择为该存储分段中的任何对象版本指定保留设置。对象版本必须具有指定的保留设置，以受 S3 对象锁定的保护。



StorageGRID S3 对象锁定功能提供了一种保留模式，相当于 Amazon S3 合规模式。默认情况下，任何用户都无法覆盖或删除受保护的对象版本。StorageGRID S3 对象锁定功能不支持监管模式，并且不允许具有特殊权限的用户绕过保留设置或删除受保护的对象。

如果存储分段启用了 S3 对象锁定，则在创建或更新对象时， S3 客户端应用程序可以选择指定以下任一或两个对象级别保留设置：

- * 保留至日期 * ：如果对象版本的保留至日期为未来日期，则可以检索该对象，但无法修改或删除它。可以根据需要增加对象的保留截止日期，但不能缩短此日期。

- * 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。

有关这些设置的详细信息、请转至中的"`使用S3对象锁定`" "S3 REST API 支持的操作和限制"。

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 NetApp 知识库文章。

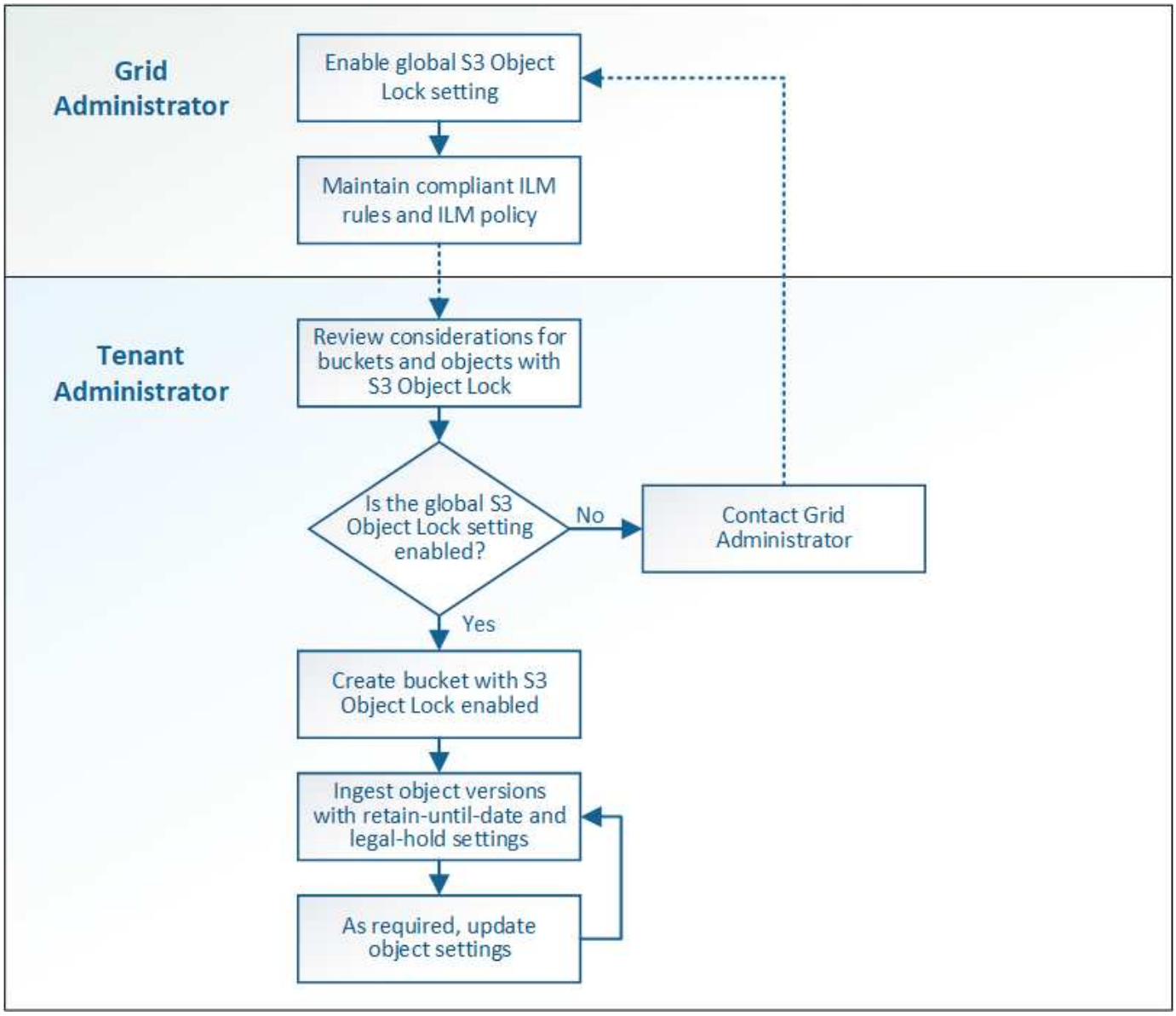
"NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

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，请联系网格管理员或查看有关通过信息生命周期管理来管理对象的说明。

启用全局 S3 对象锁定设置后，您可以在启用了 S3 对象锁定的情况下创建存储分段。然后，您可以使用 S3 客户端应用程序为每个对象版本指定保留设置。



相关信息

"使用 ILM 管理对象"

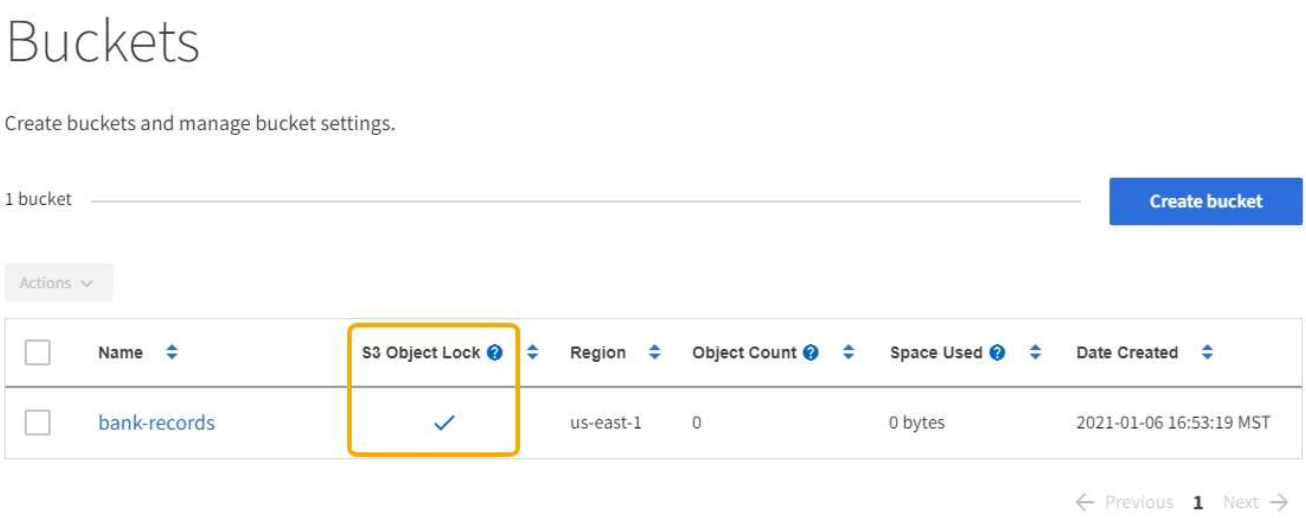
S3 对象锁定的要求

在为存储分段启用 S3 对象锁定之前，请查看 S3 对象锁定存储分段和对象的要求以及启用了 S3 对象锁定的存储分段中对象的生命周期。

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。

  此租户管理器示例显示了一个已启用 S3 对象锁定的存储分段。



- 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。
- S3 对象锁定需要分段版本。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。
- 在启用了 S3 对象锁定的情况下创建存储分段后，无法禁用 S3 对象锁定或暂停该存储分段的版本控制。
- 启用了S3对象锁定的StorageGRID 存储分段没有默认保留期限。相反、S3客户端应用程序可以选择为添加到存储分段的每个对象版本指定保留日期和合法保留设置。
- S3 对象生命周期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

- S3客户端应用程序必须为需要受S3对象锁定保护的每个对象指定保留设置。
- 您可以增加对象版本的保留截止日期，但不能减小此值。
- 如果您收到有关待定法律诉讼或监管调查的通知，则可以通过对对象版本进行法律保留来保留相关信息。如果对象版本处于合法保留状态，则无法从 StorageGRID 中删除该对象，即使该对象已达到保留日期。一旦取消合法保留，如果已达到保留日期，则可以删除对象版本。
- S3 对象锁定需要使用版本控制的分段。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

保存在启用了 S3 对象锁定的存储分段中的每个对象将经历三个阶段：

1. * 对象载入 *
    - 在启用了 S3 对象锁定的情况下，将对象版本添加到存储分段时， S3 客户端应用程序可以选择为此对象指定保留设置（ retene-until date ， legal hold 或两者）。然后， StorageGRID 会为此对象生成元数据，其中包括唯一对象标识符（ UUID ）以及载入日期和时间。
    - 载入具有保留设置的对象版本后，将无法修改其数据和 S3 用户定义的元数据。
    - StorageGRID 存储的对象元数据与对象数据无关。它会为每个站点上的所有对象元数据维护三个副本。

2. * 对象保留 *
   - StorageGRID 会存储该对象的多个副本。副本的确切数量和类型以及存储位置取决于活动 ILM 策略中的合规规则。
3. * 对象删除 *
   - 达到保留截止日期后，可以删除对象。
   - 无法删除处于合法保留状态的对象。

创建**S3**存储分段

您可以使用租户管理器为对象数据创建 S3 分段。创建存储分段时，必须指定存储分段的名称和区域。如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以选择为存储分段启用 S3 对象锁定。

您需要的内容

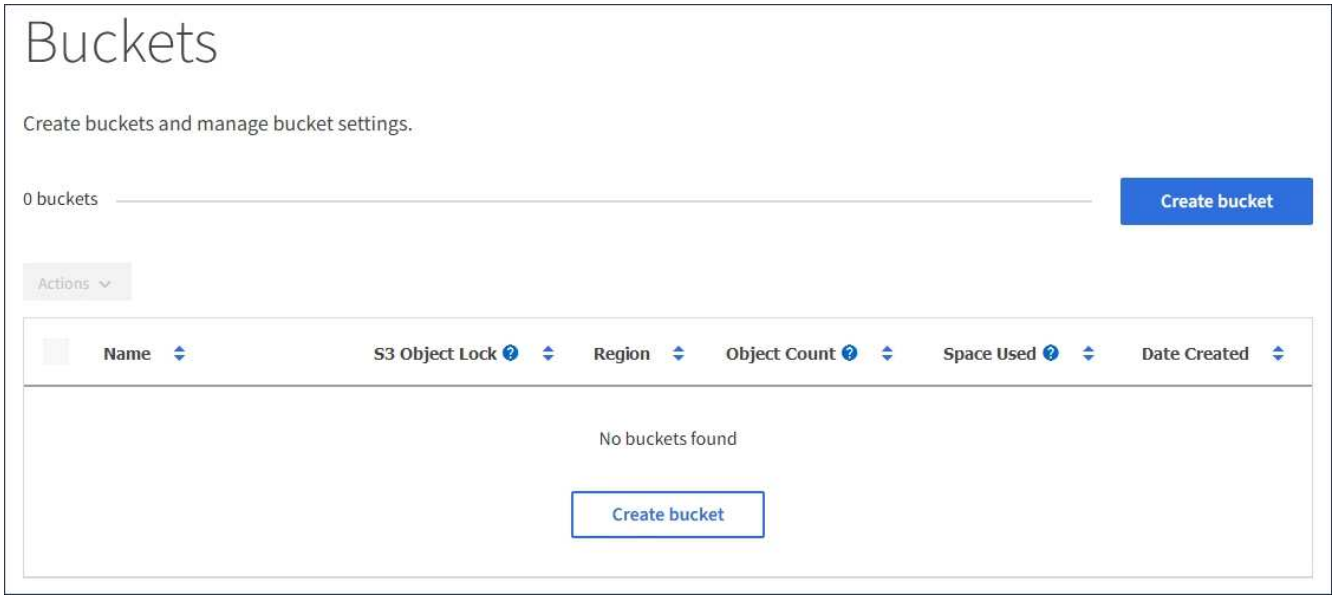
- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。
- 如果您计划使用S3对象锁定创建存储分段、则必须已为StorageGRID 系统启用全局S3对象锁定设置、并且您必须已查看S3对象锁定存储分段和对象的要求。

  "使用 S3 对象锁定"

步骤

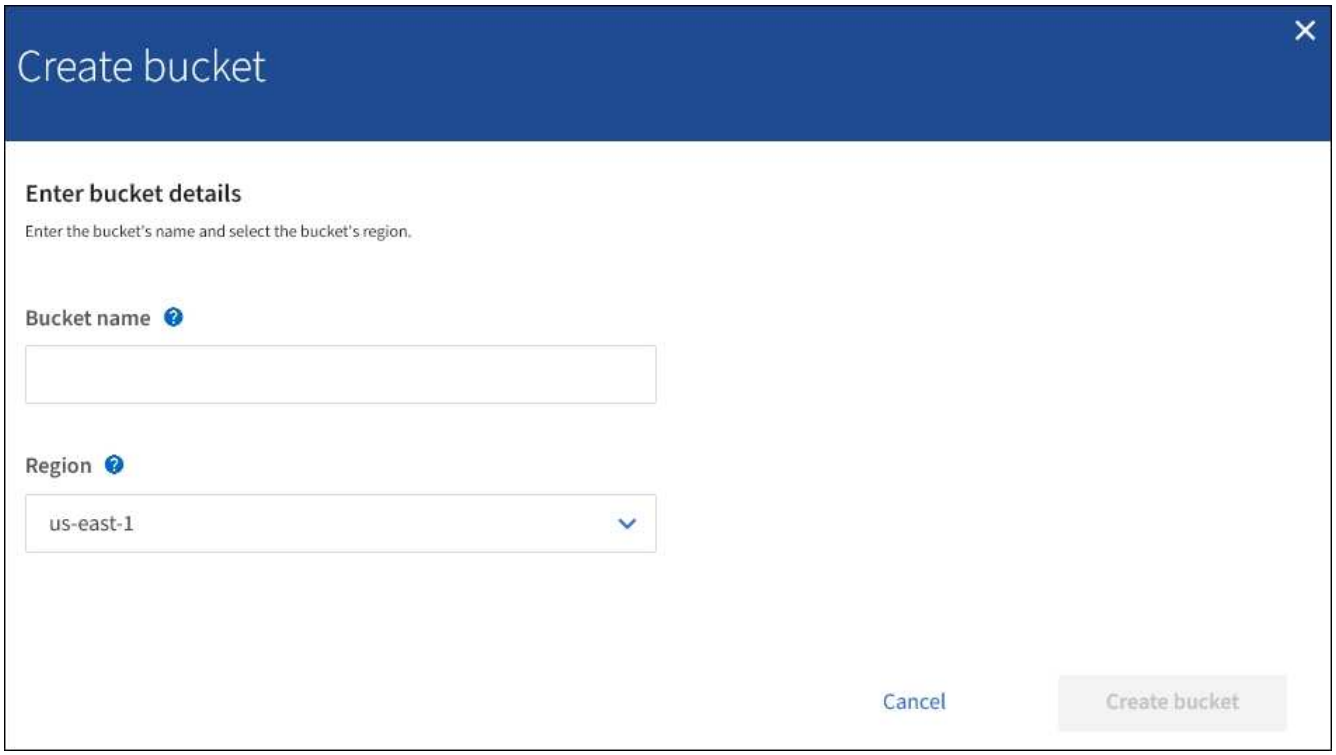
1. 选择 * 存储（ S3 ） * > * 分段 * 。

   此时将显示"分段"页面、其中列出了已创建的任何分段。



2. 选择 * 创建存储分段 * 。

   此时将显示创建存储分段向导。



如果启用了全局S3对象锁定设置、则创建存储分段包括管理存储分段的S3对象锁定的第二个步骤。

3. 输入存储分段的唯一名称。

创建存储分段后，您无法更改存储分段名称。

存储分段名称必须符合以下规则：

- 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。
- 可以是一个或多个标签的序列，并使用一个句点分隔相邻标签。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。
- 不能与文本格式的 IP 地址类似。
- 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。

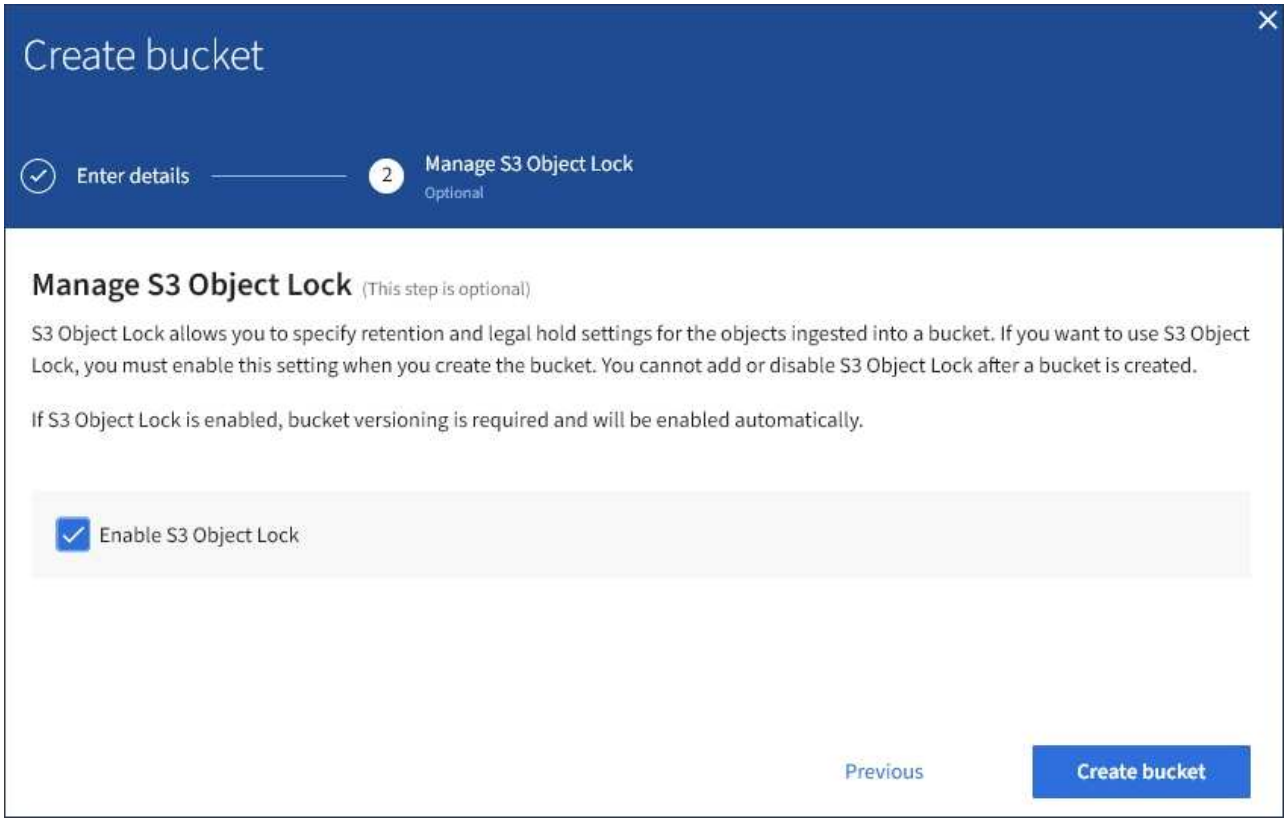
有关详细信息、请参见Amazon Web Services (AWS)文档。

4. 为此存储分段选择区域。

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。

创建存储分段后，您无法更改此区域。

5. 选择*创建存储分段*或*继续*。
   - 如果未启用全局S3对象锁定设置、请选择*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。
   - 如果启用了全局S3对象锁定设置、请选择*继续*。此时将显示第2步"管理S3对象锁定"。



6. 或者、选中此复选框以为此存储分段启用S3对象锁定。

   必须为存储分段启用 S3 对象锁定， S3 客户端应用程序才能为添加到存储分段的对象指定保留日期和合法保留设置。

   创建存储分段后，您无法启用或禁用 S3 对象锁定。

   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。

7. 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。

相关信息

"使用 ILM 管理对象"

"了解租户管理API"

"使用 S3"

查看**S3**存储分段详细信息

您可以查看租户帐户中的分段和分段设置列表。

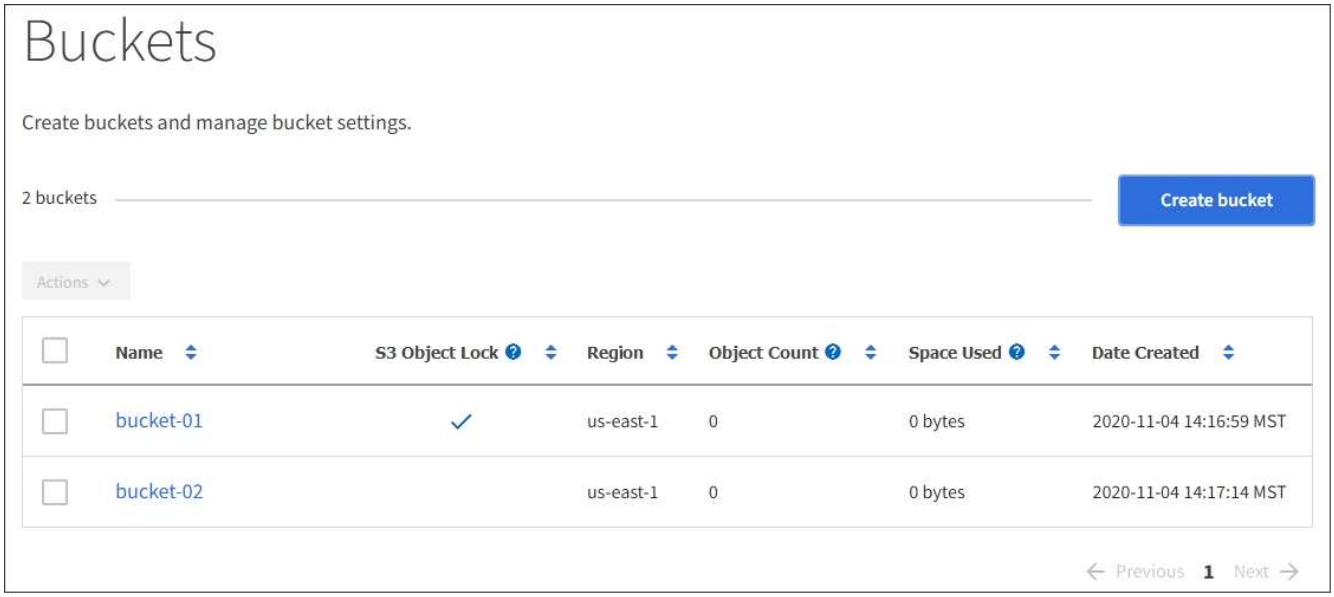
您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。

   此时将显示 " 分段 " 页面，其中列出了租户帐户的所有分段。



2. 查看每个存储分段的信息。

   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。

   - name ： 存储分段的唯一名称，不能更改。
   - S3 对象锁定：是否为此存储分段启用了 S3 对象锁定。

     如果禁用全局 S3 对象锁定设置，则不会显示此列。此列还会显示任何旧版合规存储分段的信息。

   - 区域：分段的区域，无法更改。
   - Object Count ： 此分段中的对象数。
   - 已用空间：此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。
   - Date created ： 创建存储分段的日期和时间。

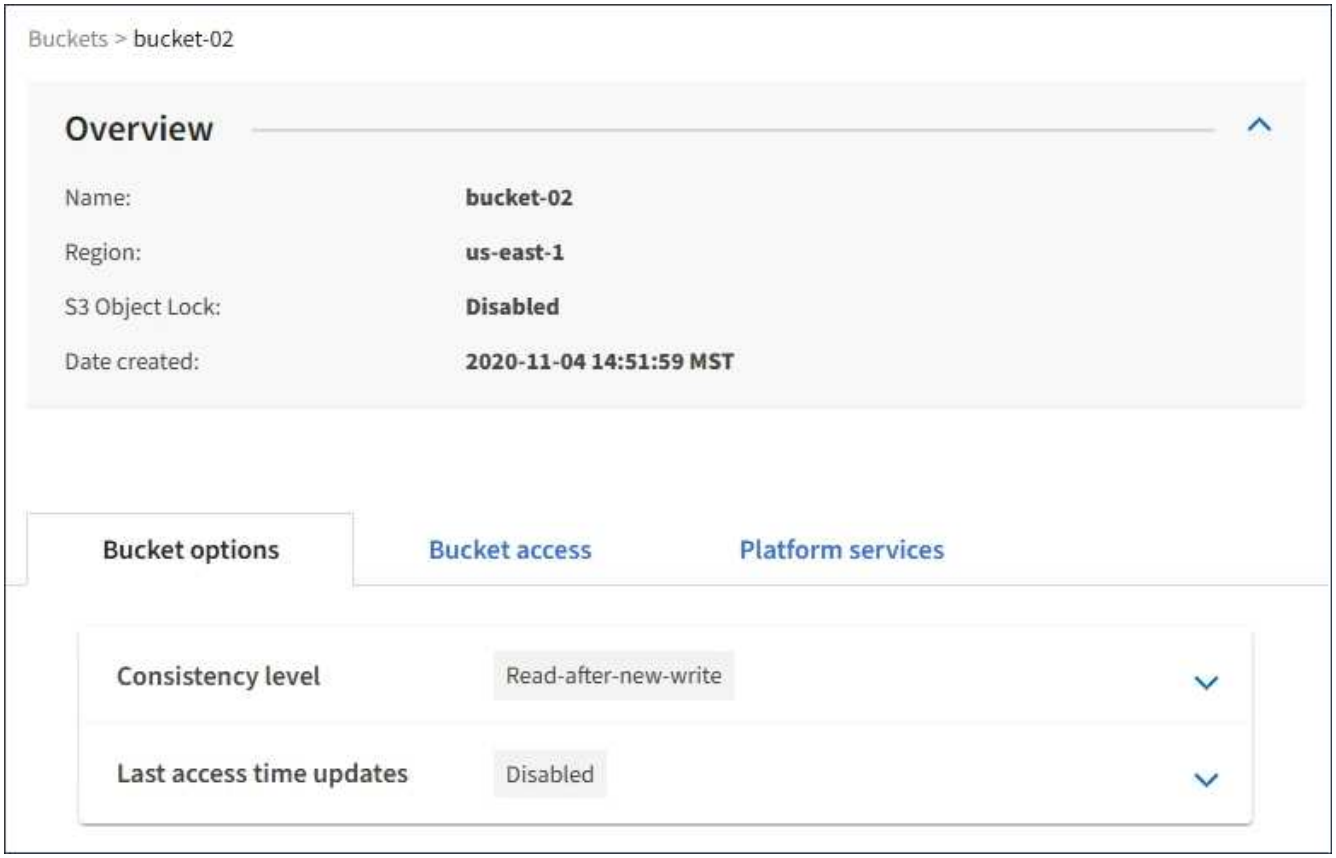
   显示的对象计数和已用空间值为估计值。这些估计值受载入时间，网络连接和节点状态的影响。

3. 要查看和管理存储分段的设置，请选择存储分段名称。

此时将显示存储分段详细信息页面。

此页面可用于查看和编辑存储分段选项、存储分段访问和平台服务的设置。

请参见有关配置每个设置或平台服务的说明。



相关信息

"更改一致性级别"

"启用或禁用上次访问时间更新"

"配置跨源资源共享(CORS)"

"配置CloudMirror复制"

"配置事件通知"

"配置搜索集成服务"

更改一致性级别

如果您使用的是 S3 租户，则可以使用租户管理器或租户管理 API 来更改对 S3 分段中的对象执行的操作的一致性控制。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。

- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。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

一致性级别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进行权衡。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。

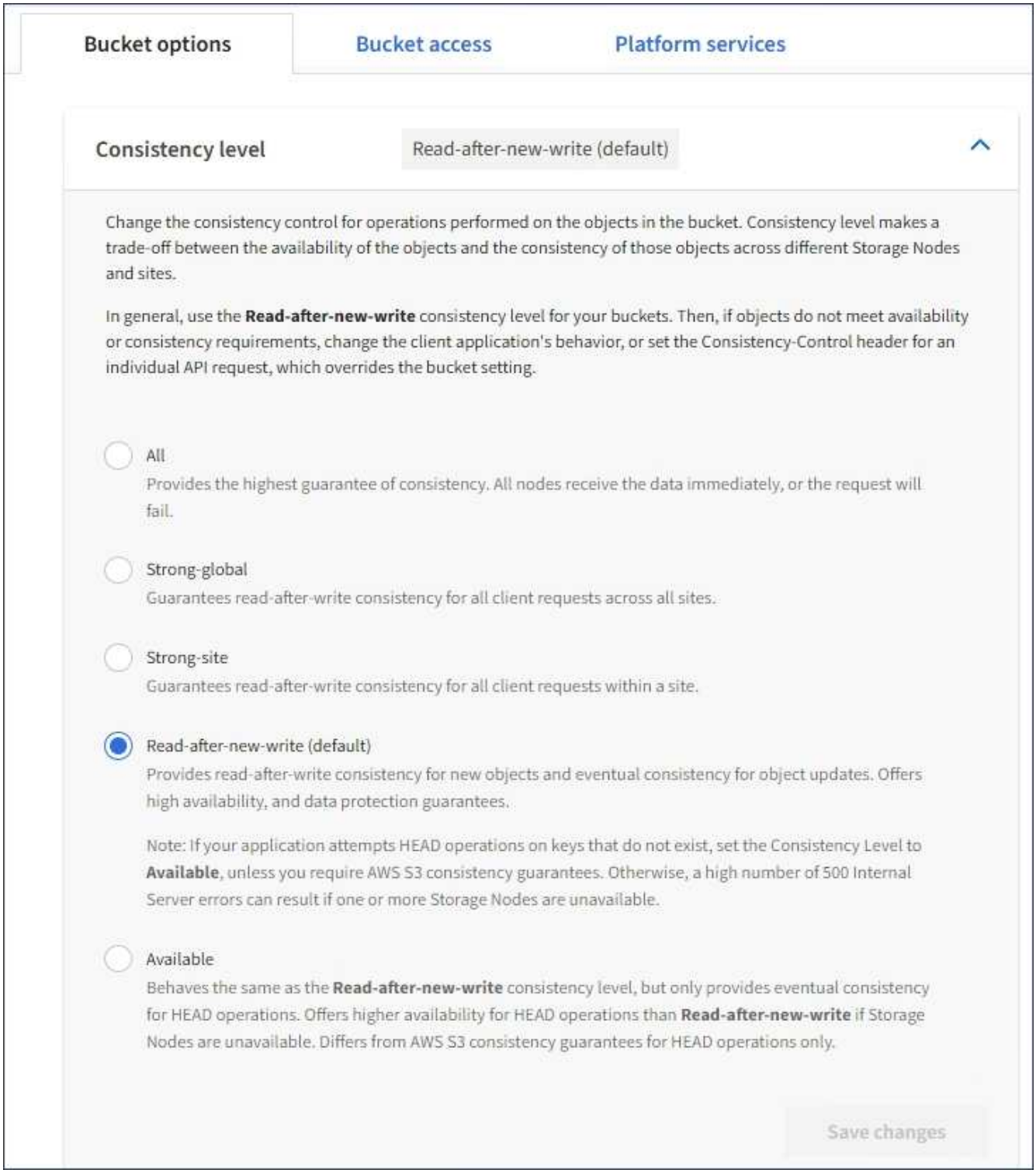
更改存储分段的一致性级别时，只会保证更改后载入的对象符合修订后的级别。

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。
2. 从列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。

3. 选择 * 分段选项 * > * 一致性级别 * 。



4. 为此存储分段中的对象选择一个一致性级别。

一致性级别	Description
全部	所有节点都会立即接收数据，否则请求将失败。
强大的全局功能	保证所有站点中所有客户端请求的写入后读一致性。

一致性级别	Description
强大的站点	保证站点内所有客户端请求的写入后读一致性。
Read-after-new-write （默认）	为新对象提供读写一致性，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。与Amazon S3一致性保证匹配。 注意：*如果应用程序尝试对不存在的密钥执行**head**操作、请将一致性级别设置为*可用、除非您需要Amazon S3一致性保证。否则，如果一个或多个存储节点不可用，则可能会出现大量 500 个内部服务器错误。
可用(机头操作的最终一致性)	与*读后新写入*一致性级别相同、但仅为机头操作提供最终一致性。如果存储节点不可用、则可为机头操作提供比*读后新写入*更高的可用性。与 Amazon S3 一致性保证不同，仅适用于机头操作。

5. 选择 * 保存更改 * 。

相关信息

"租户管理权限"

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在放置说明中使用 * 上次访问时间 * 选项的 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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。

对于 ILM 规则， * 上次访问时间 * 是 * 参考时间 * 放置说明可用的选项之一。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。

请参见有关通过信息生命周期管理来管理对象的说明。

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，并且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 存储分段启用对上次访问时间的更新。

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。

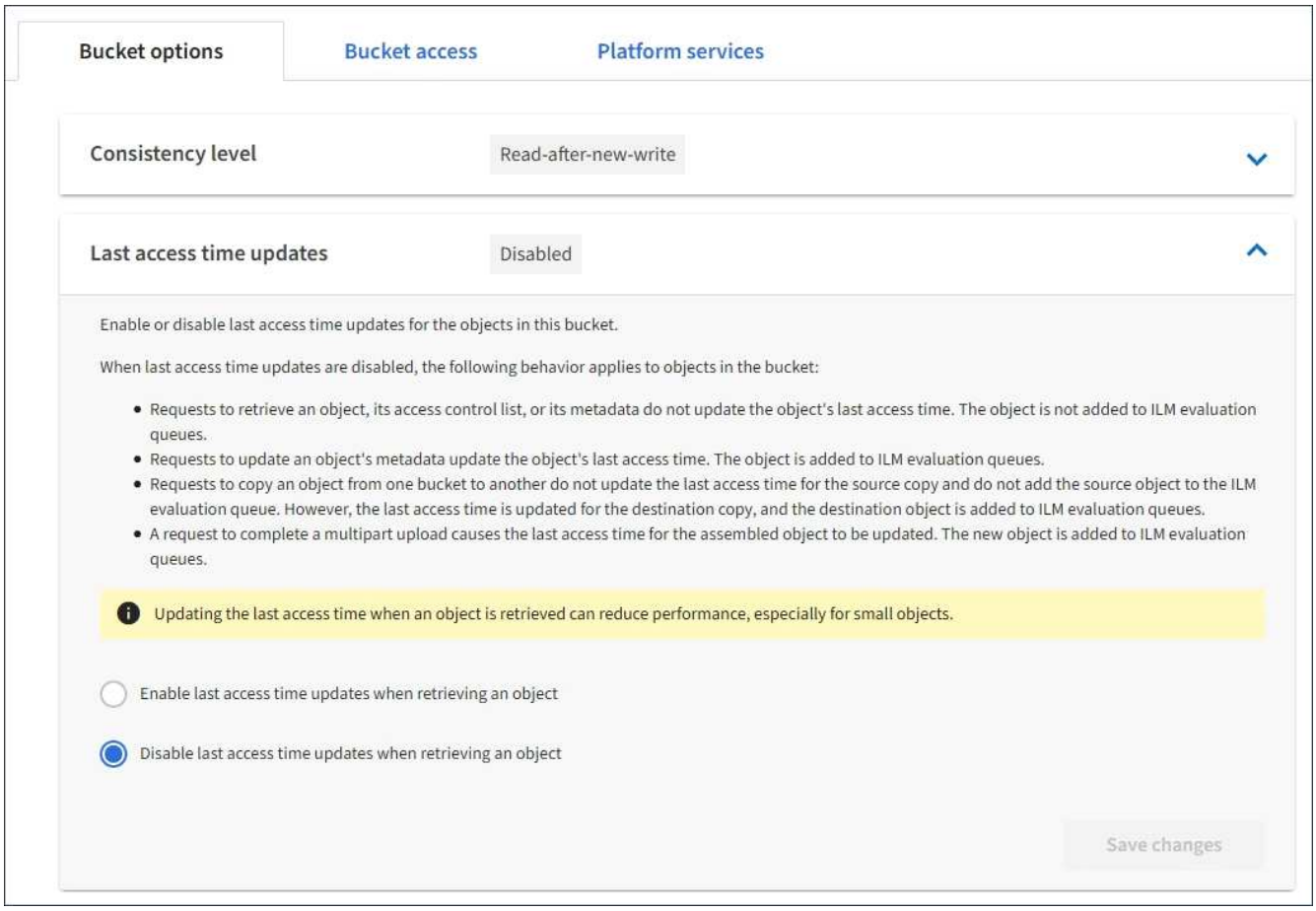
请求类型	禁用上次访问时间时的行为（默认）		启用上次访问时间时的行为	
	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?
请求检索对象，其访问控制列表或其元数据	否	否	是的。	是的。
请求更新对象的元数据	是的。	是的。	是的。	是的。
请求将对象从一个存储分段复制到另一个存储分段	• 否，对于源副本 • 是，对于目标副本	• 否，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本
请求完成多部分上传	是，对于已组装的对象	是，对于已组装的对象	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

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。
2. 从列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。

3. 选择 * 分段选项 * > * 上次访问时间更新 * 。
4. 选择相应的单选按钮以启用或禁用上次访问时间更新。



5. 选择 * 保存更改 * 。

相关信息

"租户管理权限"

"使用 ILM 管理对象"

配置跨源资源共享(CORS)

如果您希望 S3 存储分段中的存储分段和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资源共享（ CORS ）。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。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`。

步骤

1. 使用文本编辑器创建启用 CORS 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。

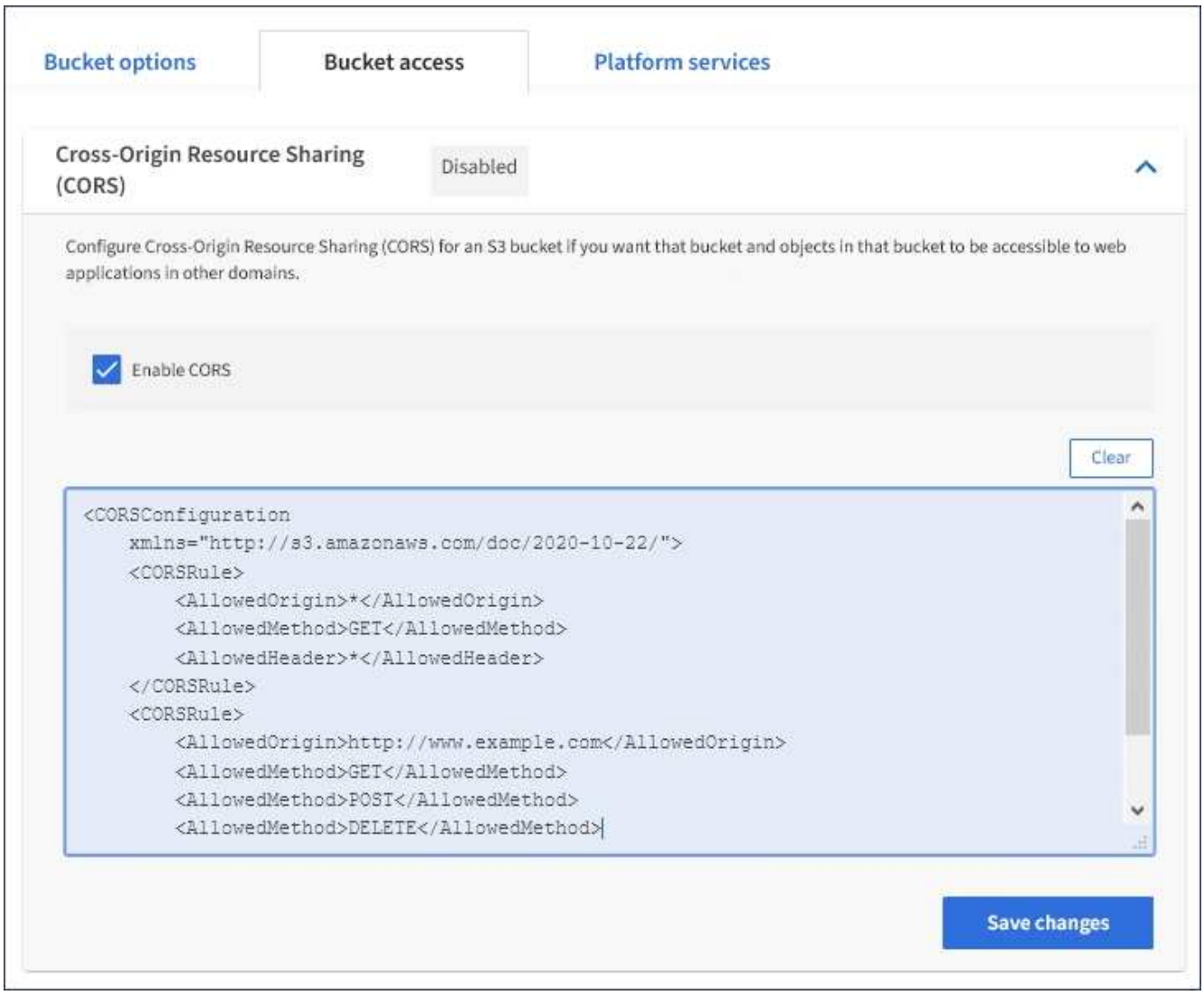
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <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. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 从列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。

4. 选择 * 分段访问 * > * 跨源资源共享（ CORS ） * 。
5. 选中 * 启用 CORS* 复选框。
6. 将 CORS 配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。



7. 要修改存储分段的 CORS 设置，请在文本框中更新 CORS 配置 XML ，或者选择 * 清除 * 重新开始。然后选择 * 保存更改 * 。
8. 要为存储分段禁用 CORS ，请取消选中 * 启用 CORS* 复选框，然后选择 * 保存更改 * 。

删除**S3**存储分段

您可以使用租户管理器删除空的 S3 存储分段。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。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

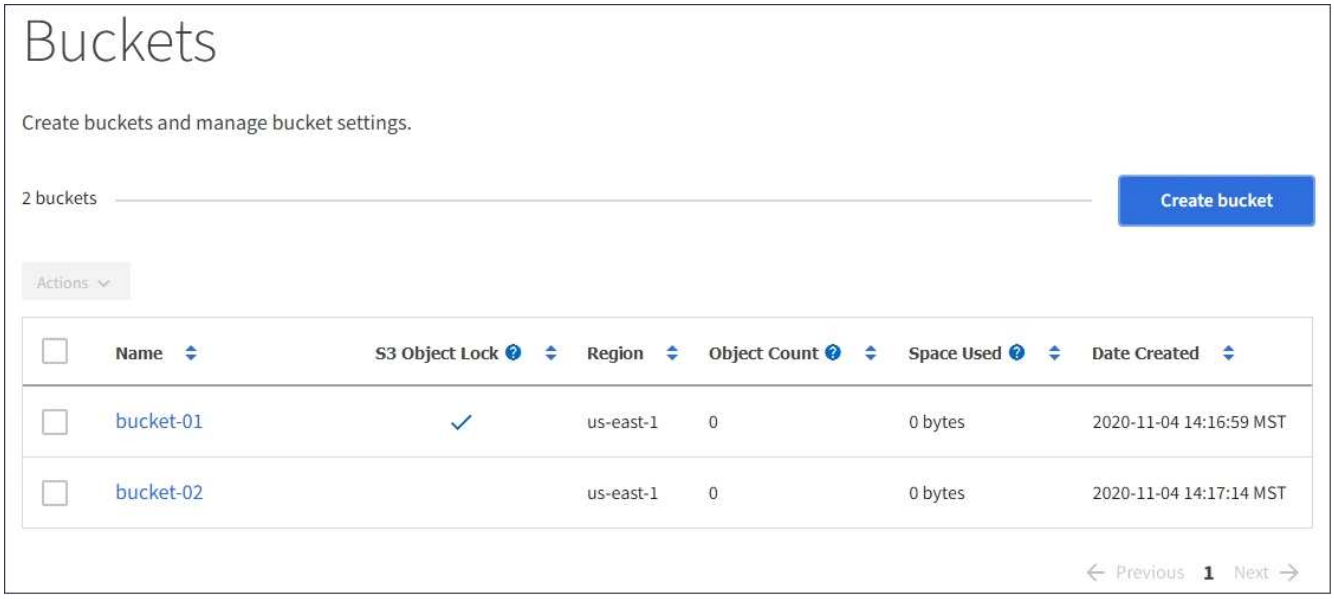
以下说明介绍如何使用租户管理器删除 S3 存储分段。您也可以使用租户管理API或S3 REST API删除S3存储分段。

如果 S3 存储分段包含对象或非当前对象版本，则不能删除该存储分段。有关如何删除S3版本对象的信息、请参见有关通过信息生命周期管理管理来管理对象的说明。

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。

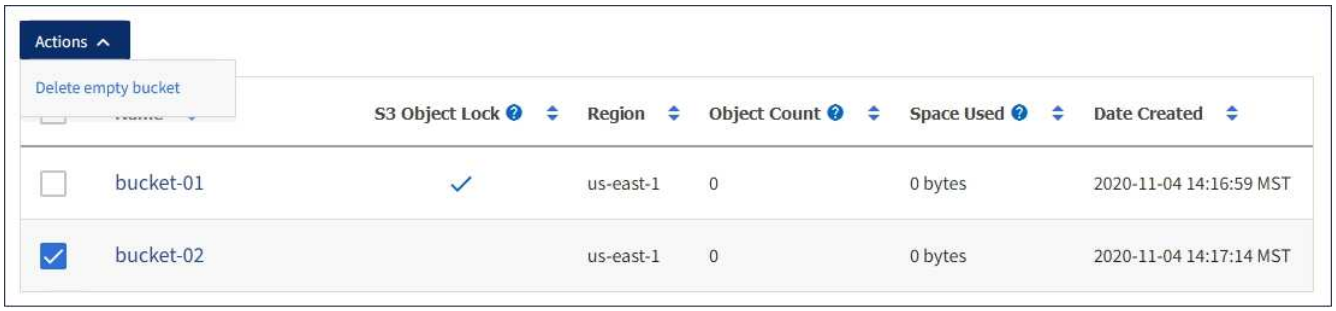
   此时将显示 " 分段 " 页面，其中会显示所有现有的 S3 分段。



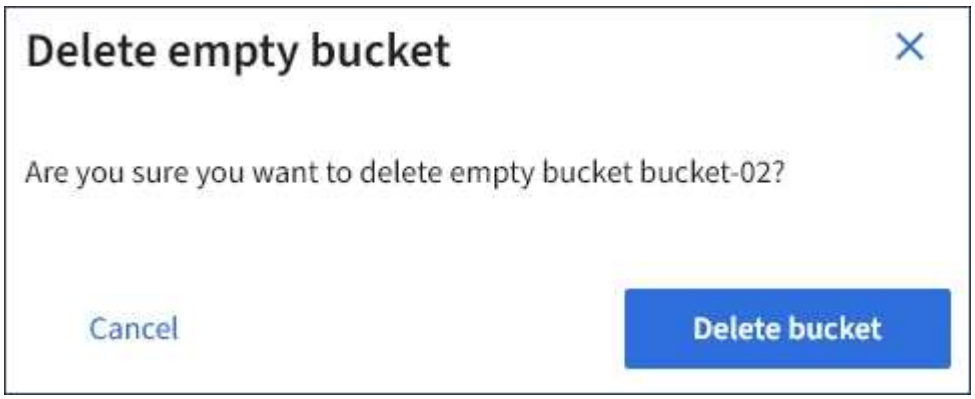
2. 选中要删除的空存储分段对应的复选框。

   此时将启用操作菜单。

3. 从操作菜单中、选择*删除空分段*。



   此时将显示一条确认消息。



4. 如果确实要删除此存储分段、请选择*删除存储分段*。

   StorageGRID 会确认此存储分段为空、然后删除此存储分段。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。必须先删除所有对象、然后才能删除此分段。

相关信息

"使用 ILM 管理对象"

管理S3平台服务

如果您的S3租户帐户允许使用平台服务、则可以使用平台服务利用外部服务并为S3存储分段配置CloudMirror复制、通知和搜索集成。

- "什么是平台服务"
- "使用平台服务的注意事项"
- "配置平台服务端点"
- "配置CloudMirror复制"
- "配置事件通知"
- "使用搜索集成服务"

什么是平台服务

StorageGRID 平台服务可以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 *： StorageGRID CloudMirror 复制服务用于将特定对象从 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 *： 每个存储分段的事件通知用于向指定的外部 Amazon Simple Notification Service （ SNS ）发送有关对对象执行的特定操作的通知。

  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 * ： 搜索集成服务用于将 S3 对象元数据发送到指定的 Elasticsearch 索引，在此索引中可以使用外部服务搜索或分析元数据。

  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

平台服务与您使用租户管理器或租户管理 API 配置的外部端点进行通信。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。

创建端点后，您可以通过向存储分段添加 XML 配置来为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：

1. 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。
2. 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。
3. 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
通知	• 获取存储分段通知 • PUT 存储分段通知

平台服务	**S3 REST API**
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。

有关 StorageGRID 如何实施这些 API 的详细信息，请参见有关实施 S3 客户端应用程序的说明。

相关信息

"使用 S3"

"了解CloudMirror复制服务"

"了解存储分段通知"

"了解搜索集成服务"

"使用平台服务的注意事项"

了解**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。

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 AWS S3 目标，请注意 Amazon S3 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。不能将对象同时复制到多个存储分段。

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 确实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。

相关信息

"配置CloudMirror复制"

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。

您可以通过将通知配置XML与源存储分段关联来配置事件通知。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 ，但存在以下限制：

- 您不能为以下事件类型配置通知。这些事件类型 * 不 * 受支持。
  - `s3:ReducedRedundancyLostObject`
  - `s3:ObjectRestore:Completed`
- 从 StorageGRID 发送的事件通知使用标准 JSON 格式，只是它们不包含某些密钥，而对其他密钥使用特定值，如下表所示：

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

密钥名称	**StorageGRID** 值
ARN	`urn:sgws:s3:::bucket_name`

相关信息

"配置事件通知"

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，您无法在索引中编辑文档的字段类型。

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_Interoperability Matrix Tool_确定支持的Elasticsearch 版本。

相关信息

"NetApp 互操作性表工具"

"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"

使用平台服务的注意事项

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。

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，如果因 StorageGRID ILM 规则而删除源存储分段中的对象，则不会发送 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存储分段的对象的最大大小为5 TB、与StorageGRID 支持的最大对象大小相同。
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 服务会复制不指定版本 ID 的 PUT 对象标记请求或删除对象标记请求。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、则复制操作将失败、并显示AccessDenied错误。

相关信息

"使用 S3"

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，并且此用户所在的网格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S3存储分段、则可以创建一个平台服务端点、其中包含StorageGRID 访问AWS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（ SQS ）或 AWS Lambda 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 Elasticsearch 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，您无需创建类型。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"

指定平台服务端点的**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：

- 如果此服务托管在AWS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上托管的服务的**urns**

对于AWS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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须属于具有管理端点权限的用户组。
- 必须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。
- 您必须具有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 ）

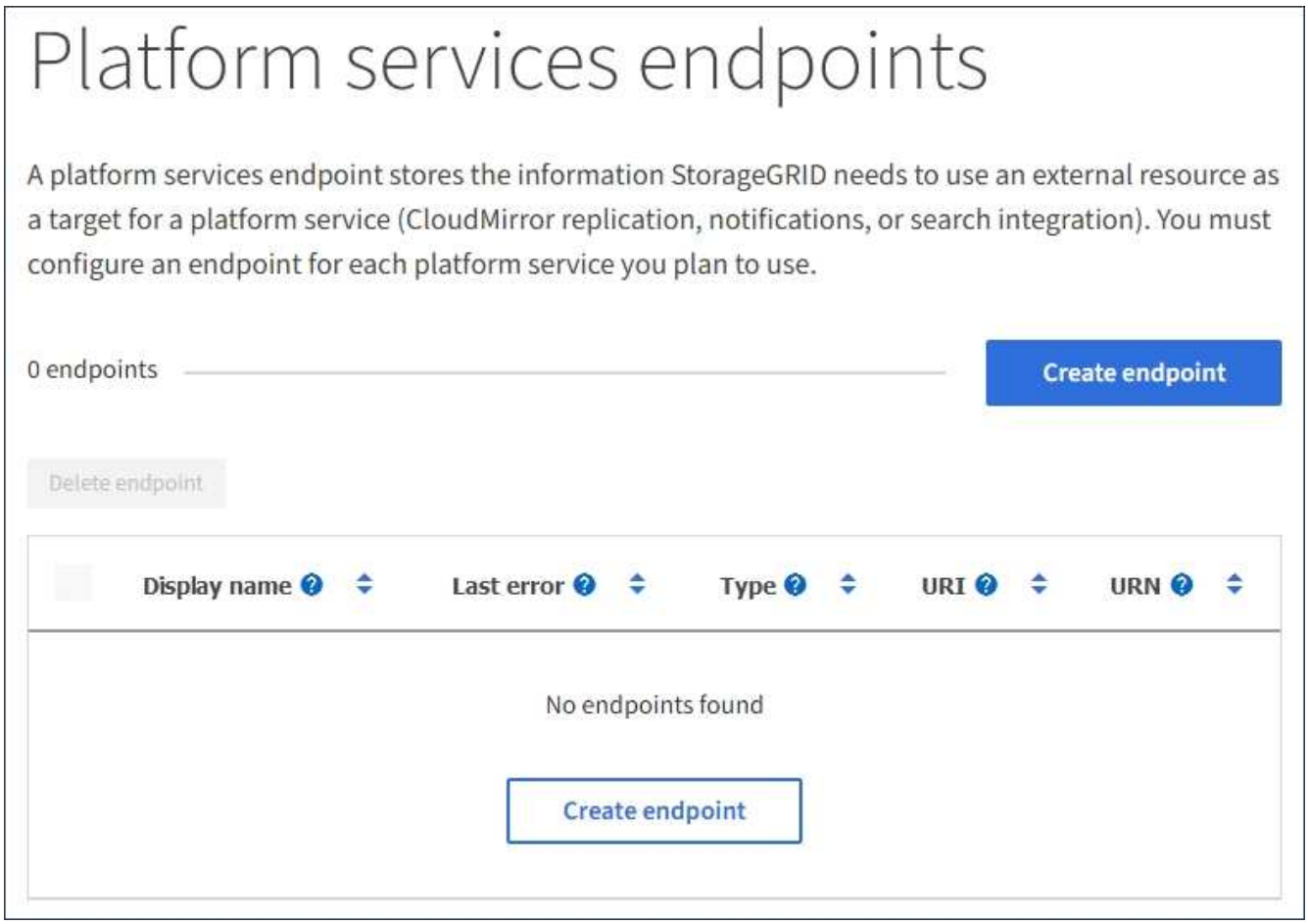
  "指定平台服务端点的URN"

- 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
- 安全证书（如果使用自定义 CA 证书）

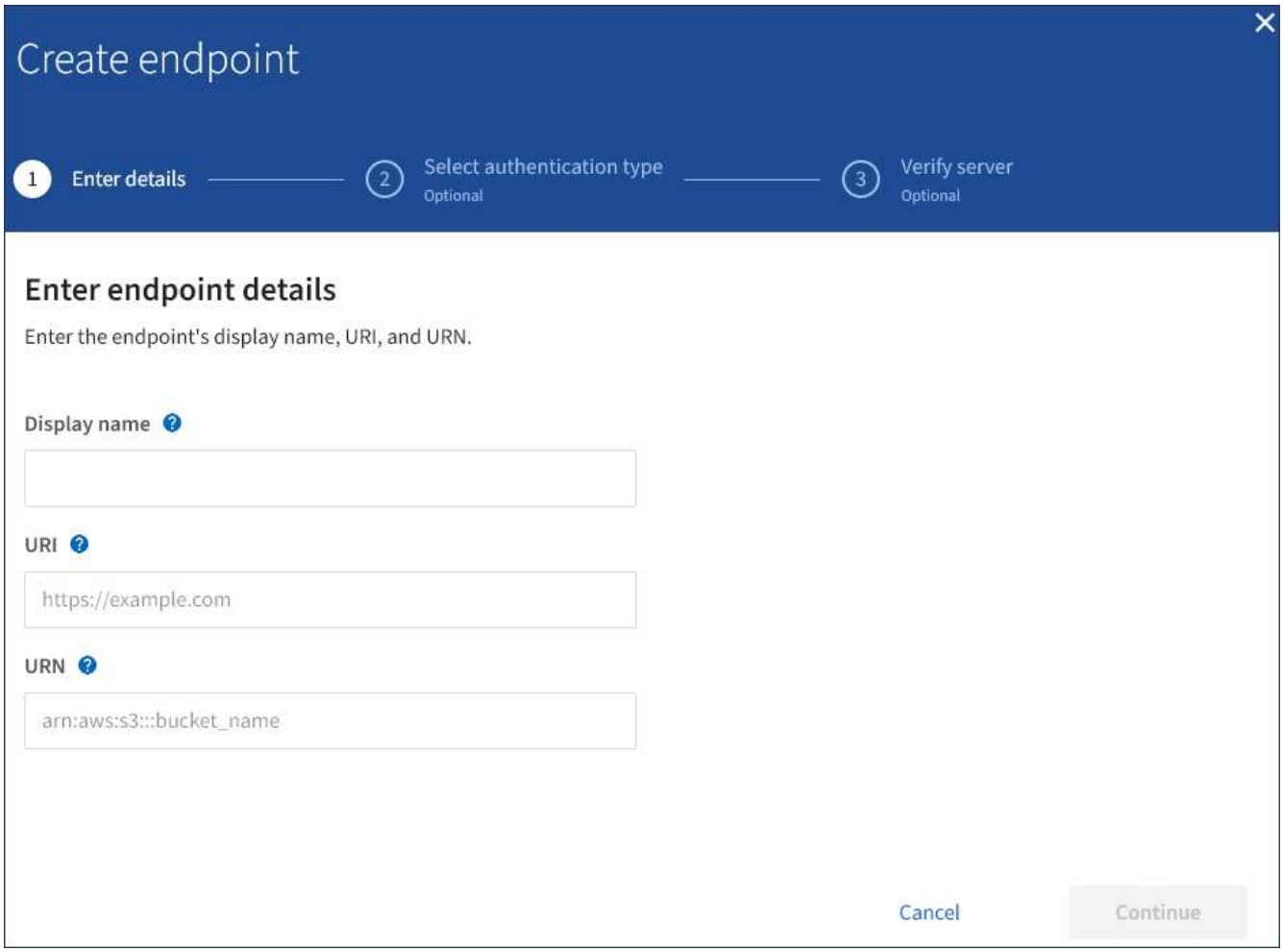
步骤

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。

   端点支持的平台服务类型会显示在端点页面上列出的端点名称旁边，因此您无需在此名称中包含此信息。

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 URI ，端口 80 用于 HTTP URI 。

   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：

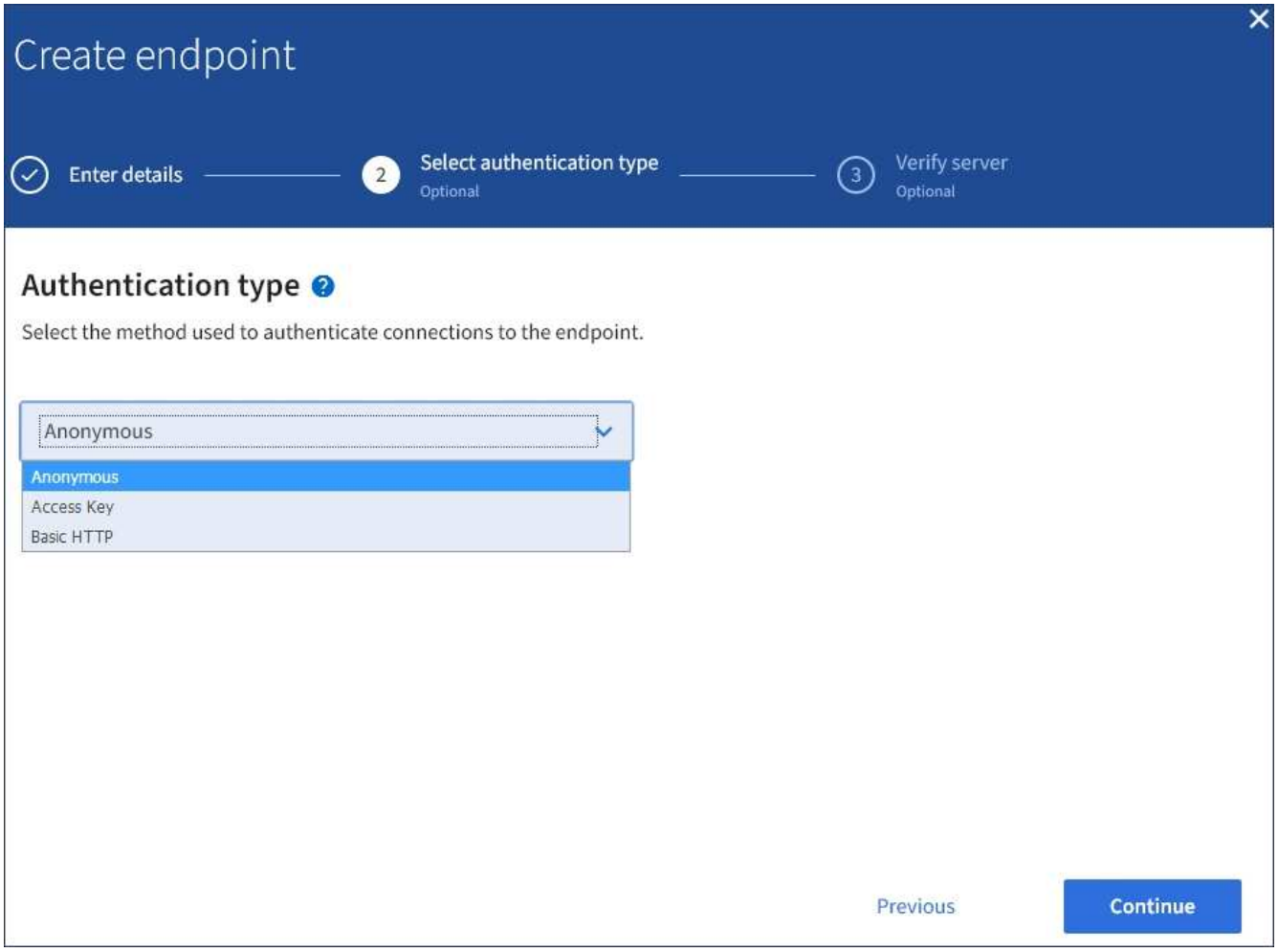
```
https://s3-aws-region.amazonaws.com
```

如果端点用于 CloudMirror 复制服务，请勿在 URI 中包含分段名称。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 。

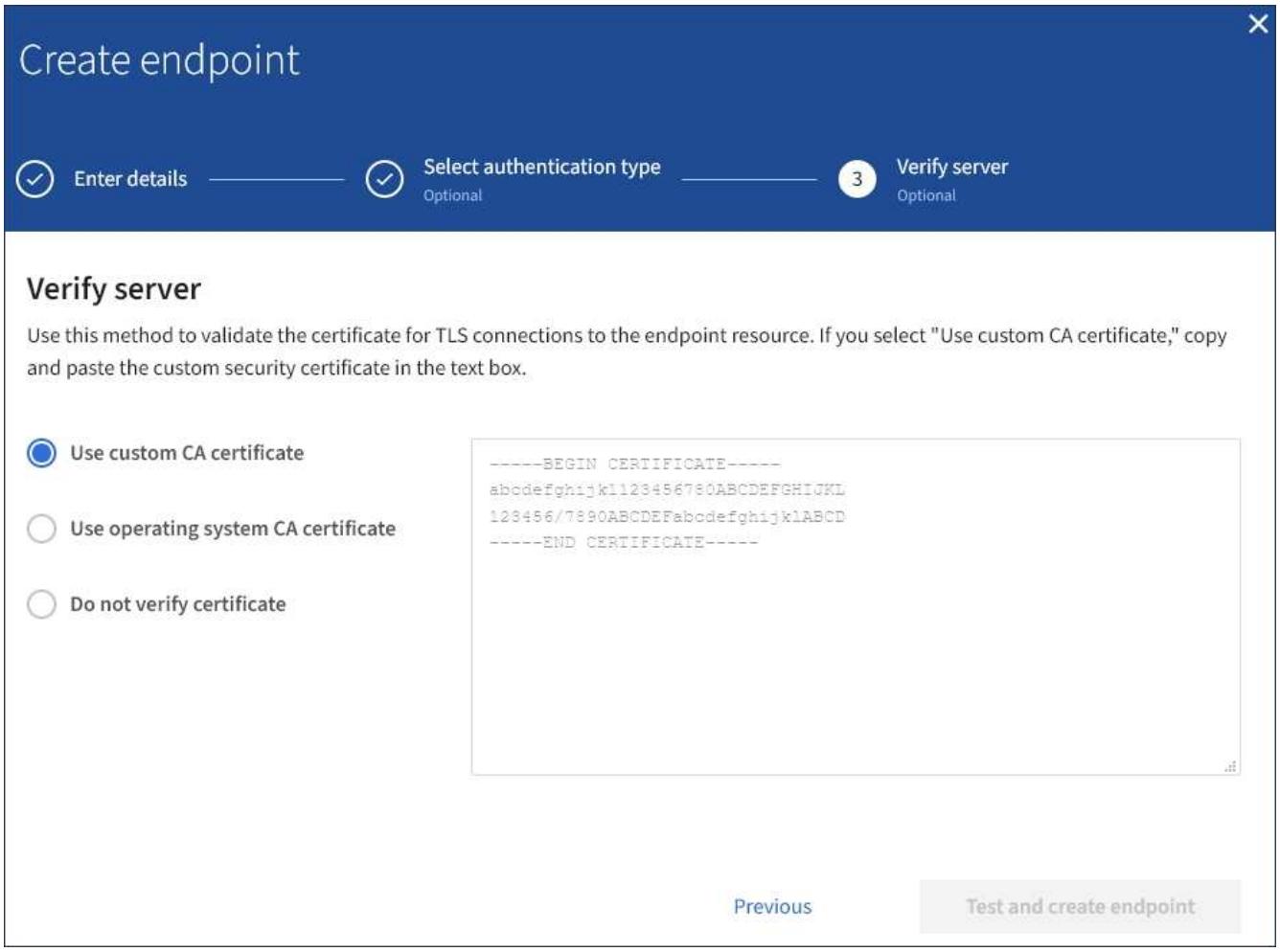
6. 选择 * 继续 * 。
7. 为*身份验证类型*选择一个值、然后输入所需的凭据。



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

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。

证书验证的类型	Description
使用操作系统 CA 证书	使用操作系统上安装的默认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

"指定平台服务端点的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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有管理端点权限的用户组。

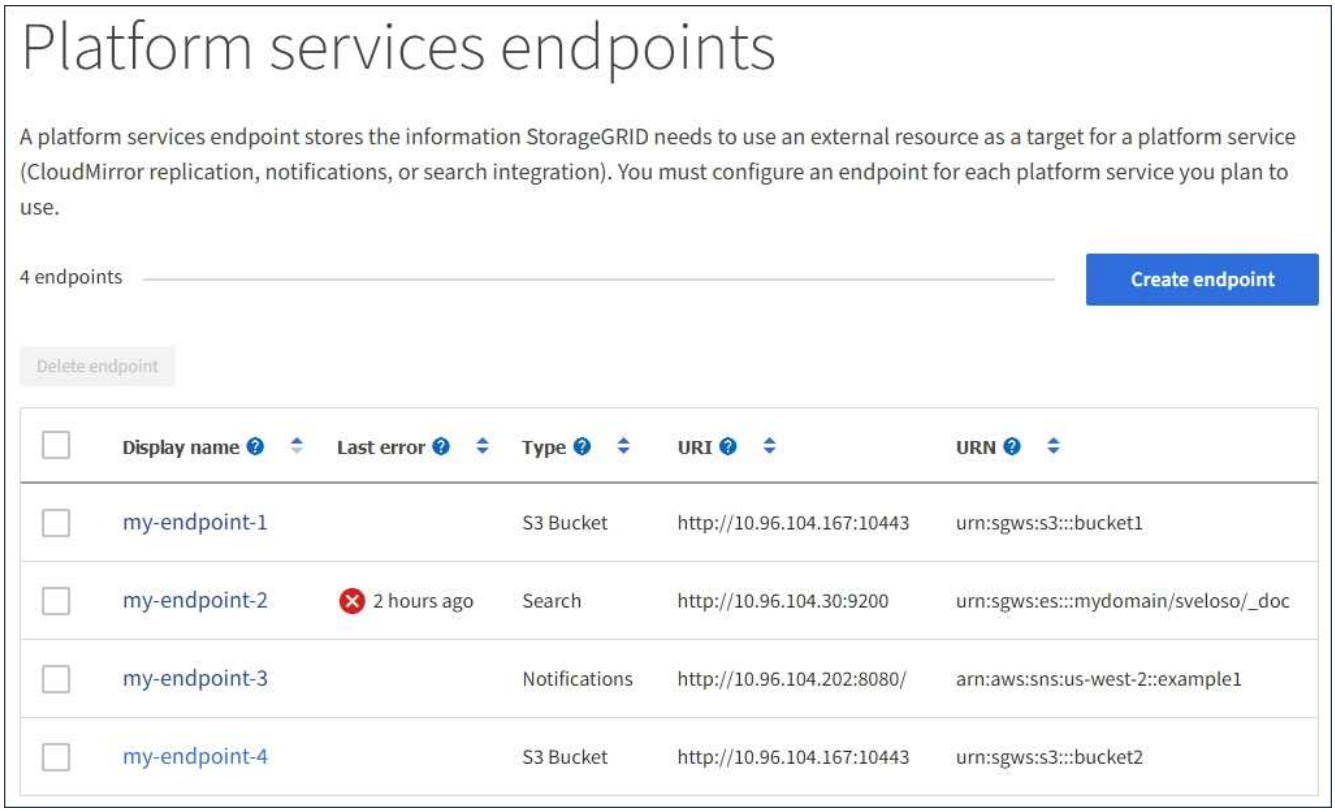
关于此任务

StorageGRID 不会验证这些凭据是否具有正确的权限。

步骤

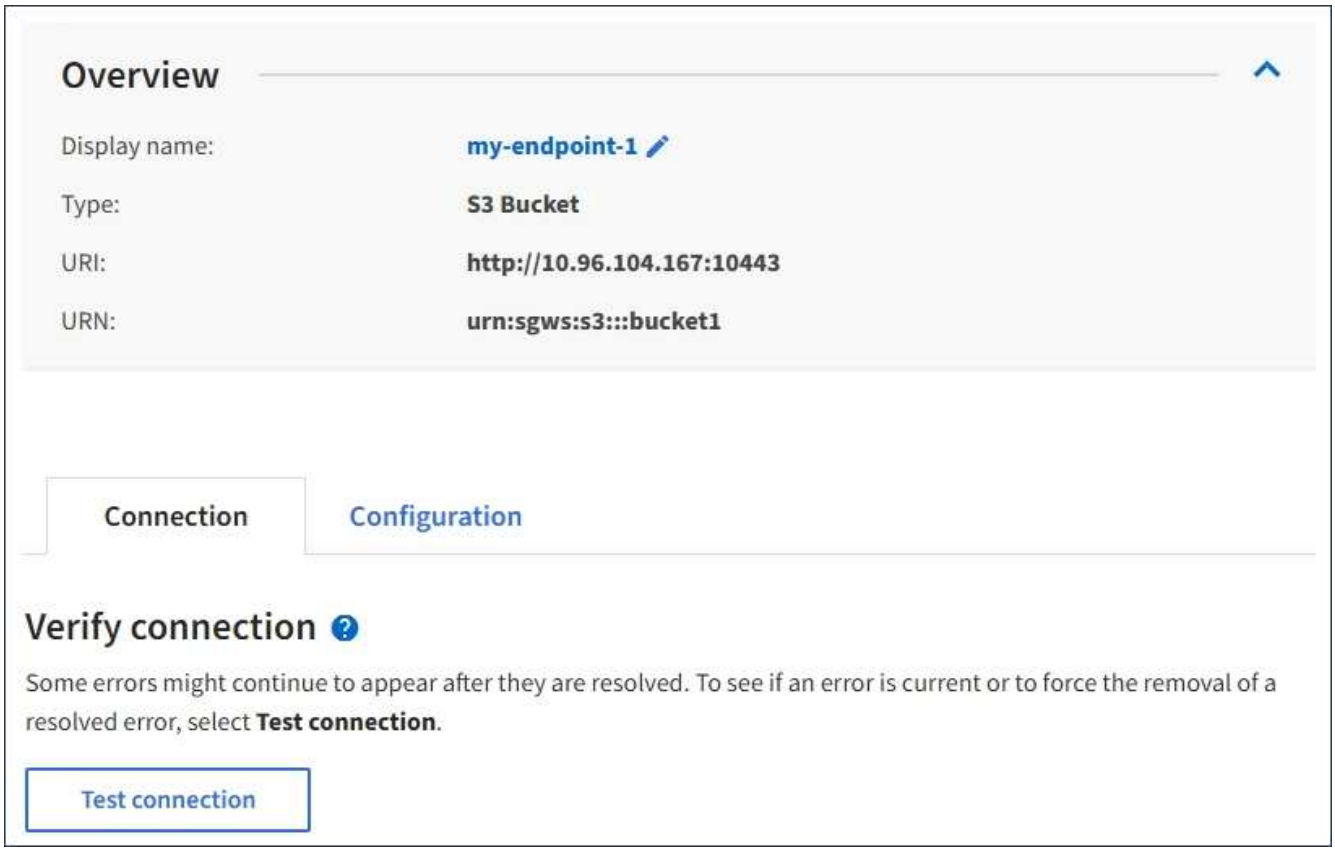
1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   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 。

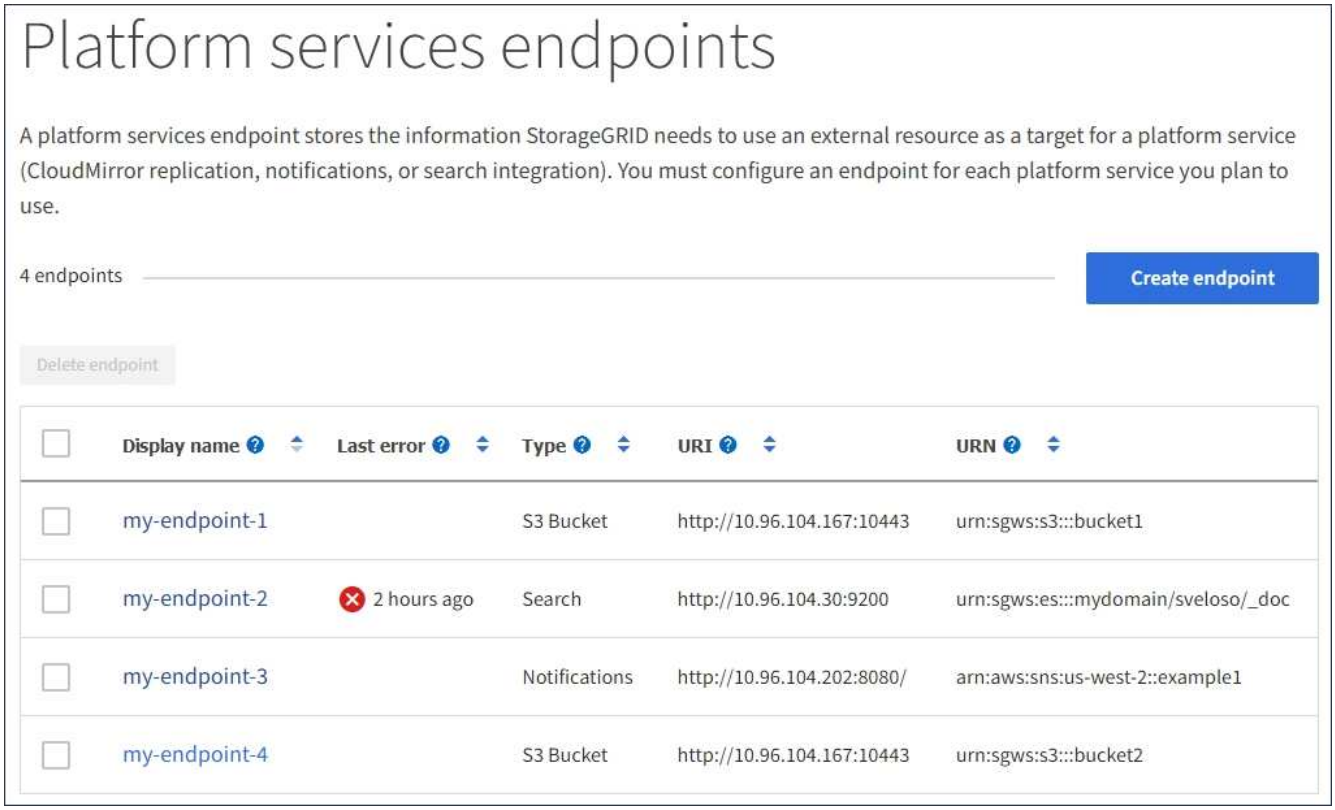
您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有管理端点权限的用户组。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

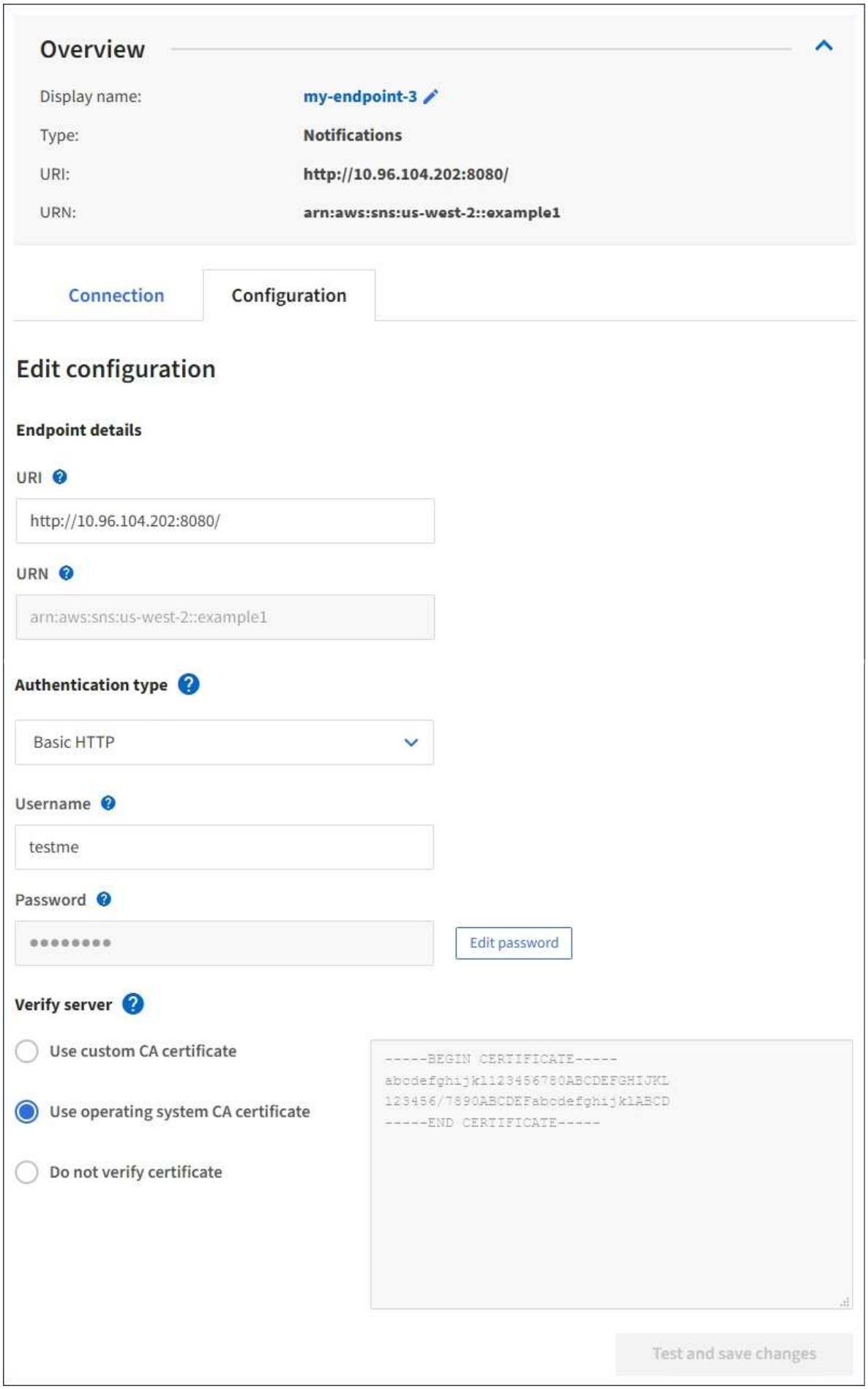
   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。



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 * 。

   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 * 。

相关信息

"创建平台服务端点"

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。

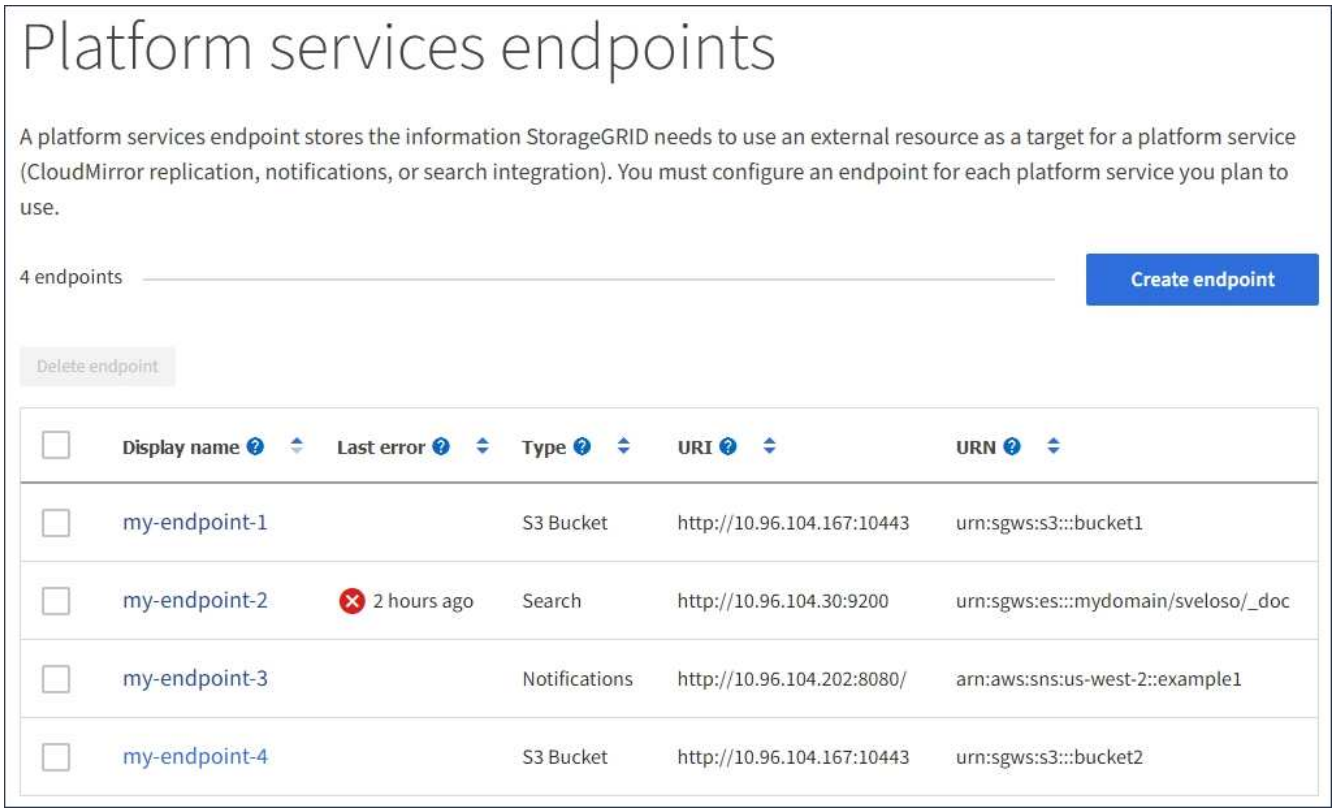
您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 * 管理端点 * 权限的用户组。

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。

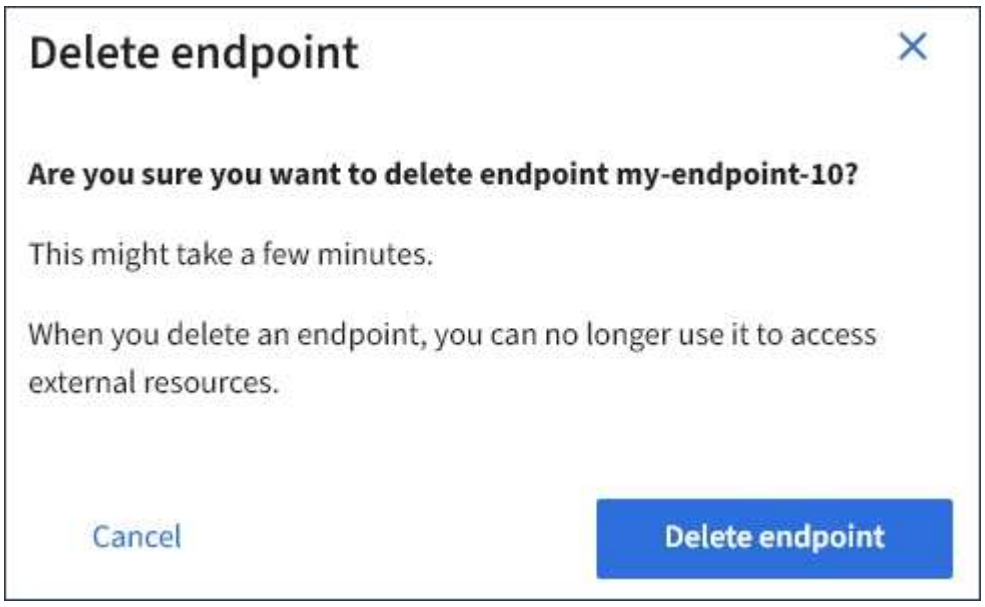


2. 选中要删除的每个端点对应的复选框。

> 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。

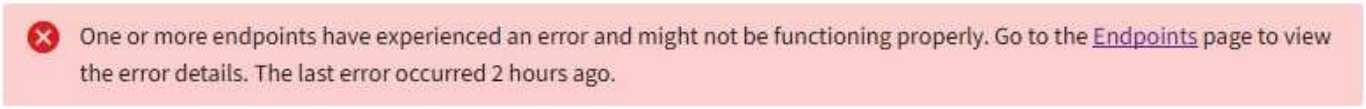


4. 选择 * 删除端点 * 。

如果在 StorageGRID 尝试与平台服务端点通信时发生错误，信息板上将显示一条消息。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

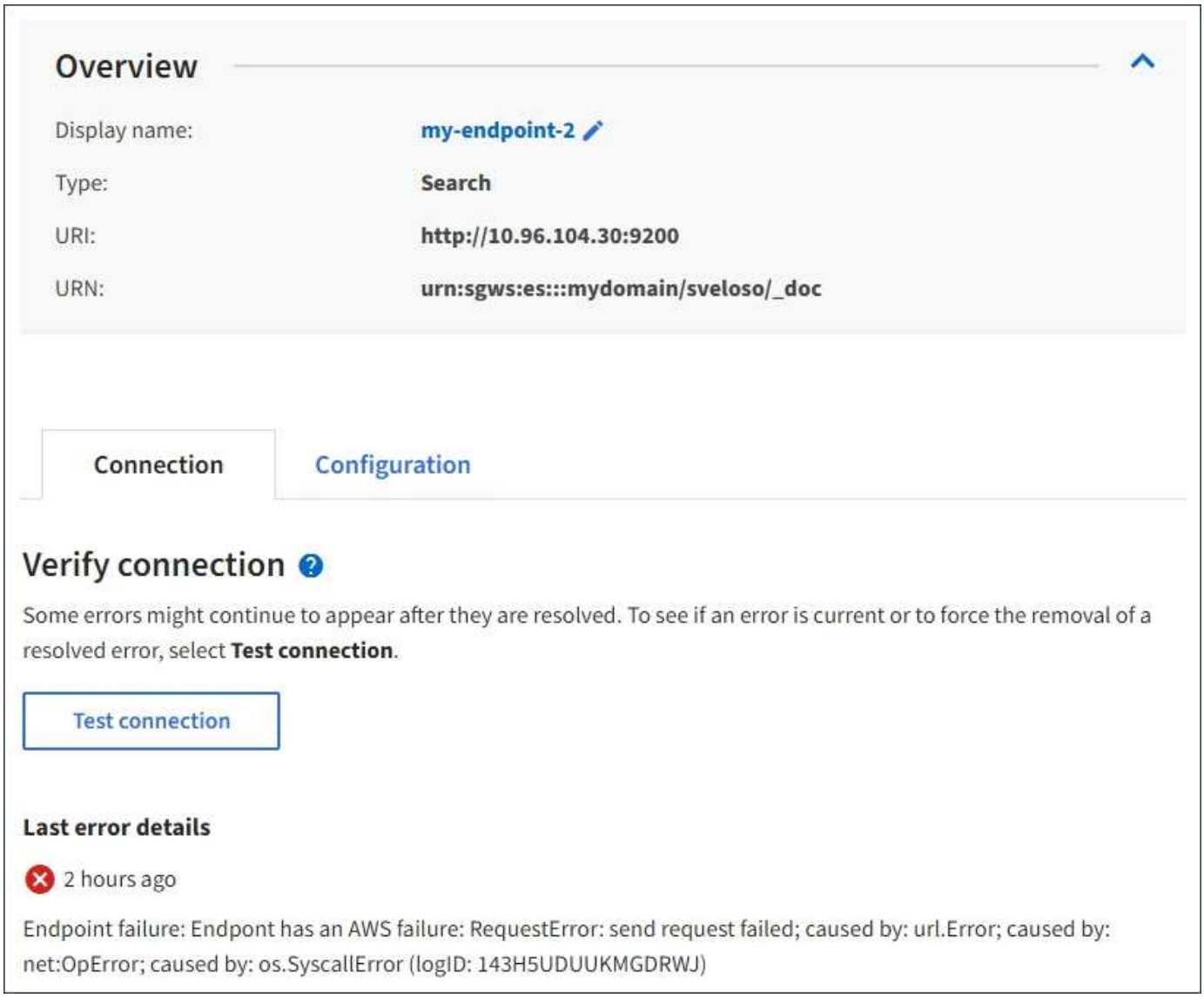
如果在过去 7 天内发生任何平台服务端点错误，则租户管理器信息板将显示一条警报消息。您可以转到平台服务端点页面以查看有关此错误的更多详细信息。



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。



检查错误是否仍为最新

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以下错误：、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。

其他平台服务故障排除

有关追加信息 对平台服务进行故障排除的信息，请参见有关管理 StorageGRID 的说明。

"管理 StorageGRID"

相关信息

"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。

您需要的内容

- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须已创建一个分段，才能用作复制源。
- 要用作 CloudMirror 复制目标的端点必须已存在，并且必须具有其 URN 。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组，此权限允许您管理租户帐户中所有 S3 分段的设置。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。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。

有关存储分段复制及其配置方法的一般信息、请参见Amazon文档中有关跨区域复制(CRR)的内容。有关StorageGRID 如何实施S3存储分段复制配置API的信息、请参见实施S3客户端应用程序的说明。

如果在包含对象的存储分段上启用 CloudMirror 复制，则会复制添加到存储分段中的新对象，但不会复制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：

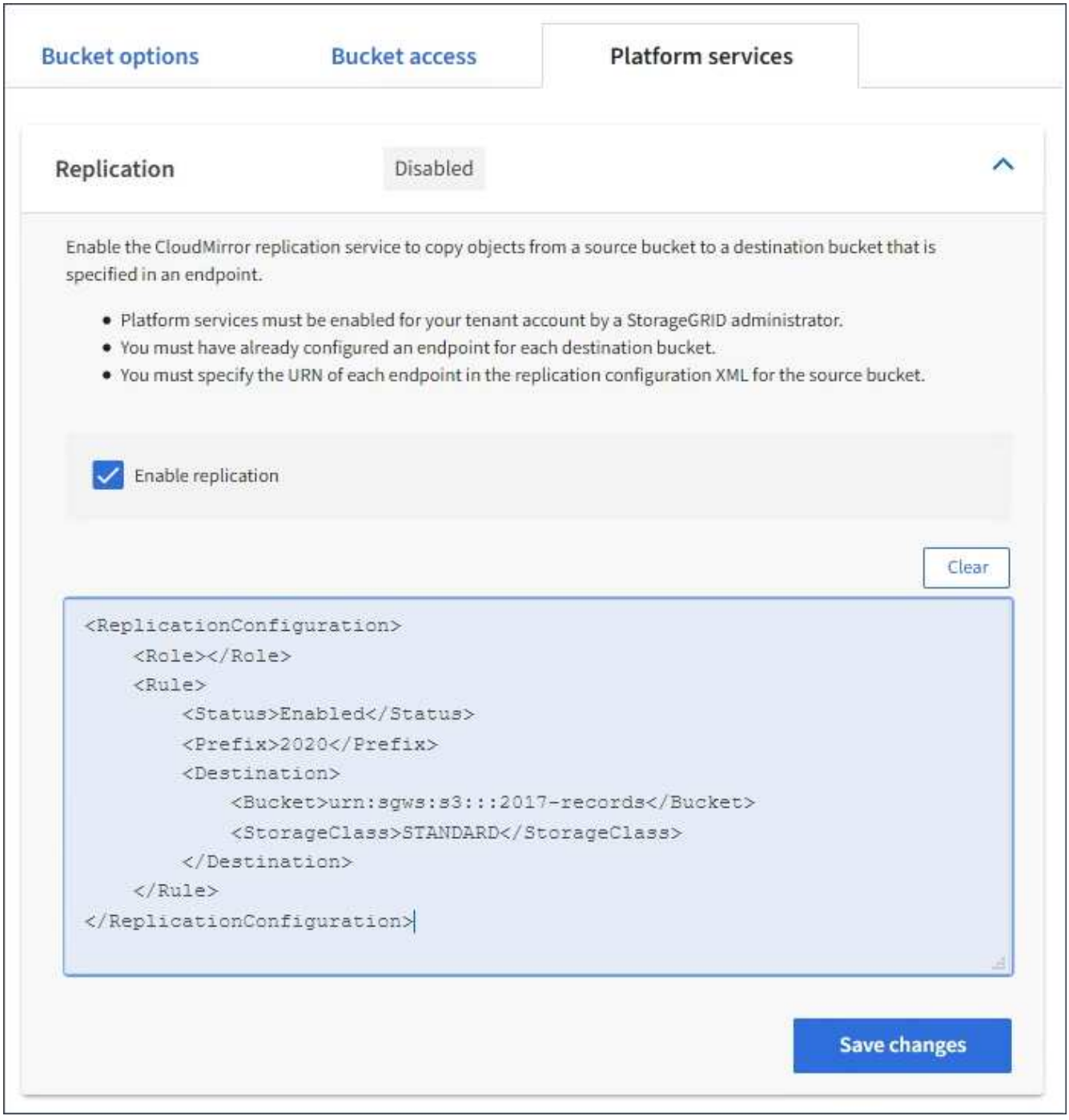
   - 请注意， StorageGRID 仅支持复制配置的 V1 。这意味着、StorageGRID 不支持使用 `Filter` Element 中的规则、并遵循V1中有关删除对象版本的约定。有关详细信息，请参见有关复制配置的 Amazon 文档。
   - 使用 S3 存储分段端点的 URN 作为目标。
   - 也可以添加 `<StorageClass>` 元素、并指定以下项之一：
     - `STANDARD`：默认存储类。如果上传对象时未指定存储类、则会显示 `STANDARD` 已使用存储类。
     - `STANDARD_IA`：(标准—不常访问。)对于访问频率较低但仍需要在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. 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 * > * 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

"了解CloudMirror复制服务"

"使用 S3"

"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。

您需要的内容

- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须已创建一个存储分段，才能用作通知源。
- 要用作事件通知目标的端点必须已存在，并且必须具有其 URN 。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组，此权限允许您管理租户帐户中所有 S3 分段的设置。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一般信息，请参见 Amazon 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：

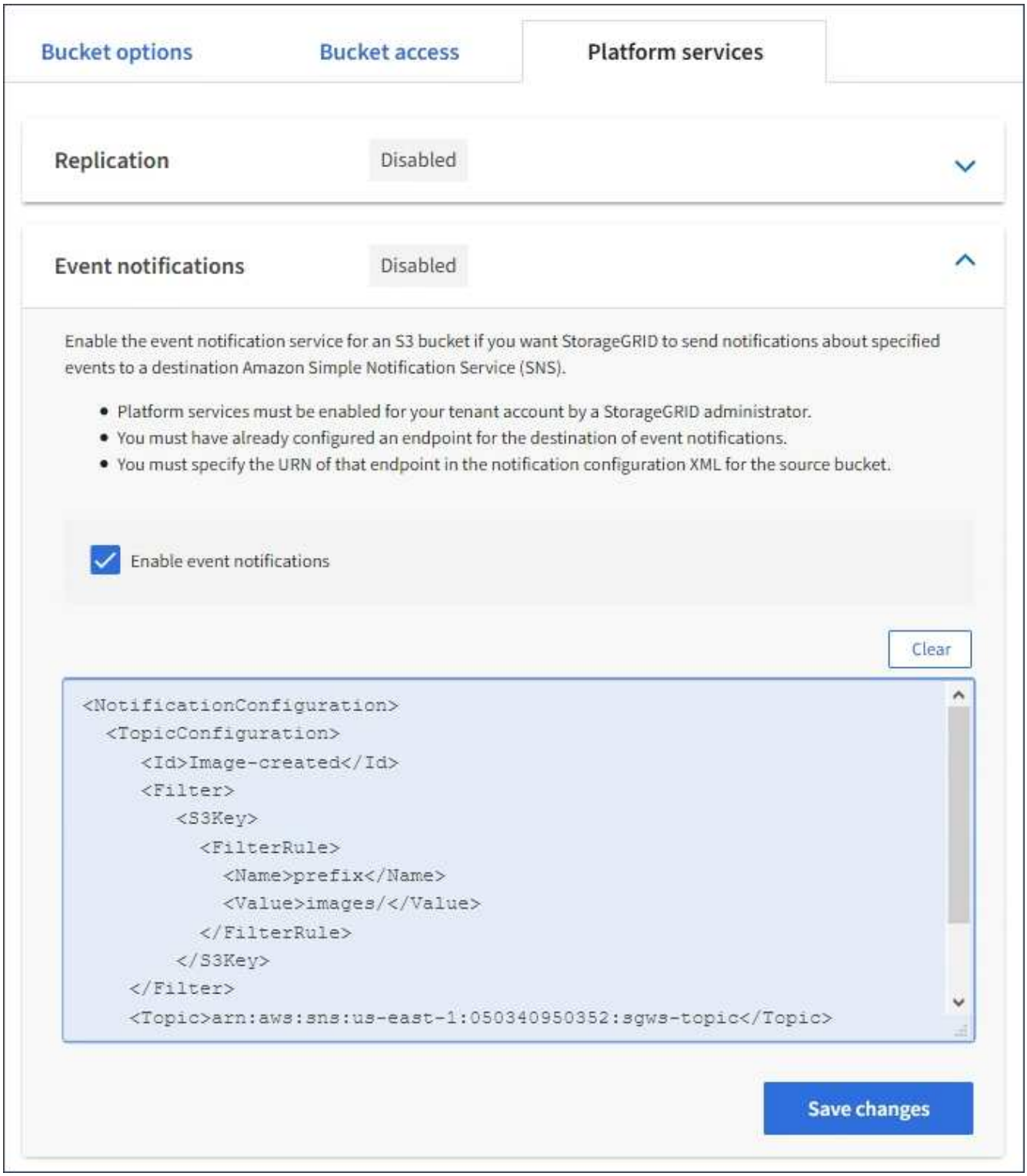
   - 使用文本编辑器创建启用 S3 通知 API 中指定的事件通知所需的通知配置 XML 。
   - 配置 XML 时，请使用事件通知端点的 URN 作为目标主题。

```
<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"

"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。

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

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

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"

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，在提交时会被拒绝。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"

"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。

您需要的内容

- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须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必须已存在，并且必须具有其 URN 。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组，此权限允许您管理租户帐户中所有 S3 分段的设置。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

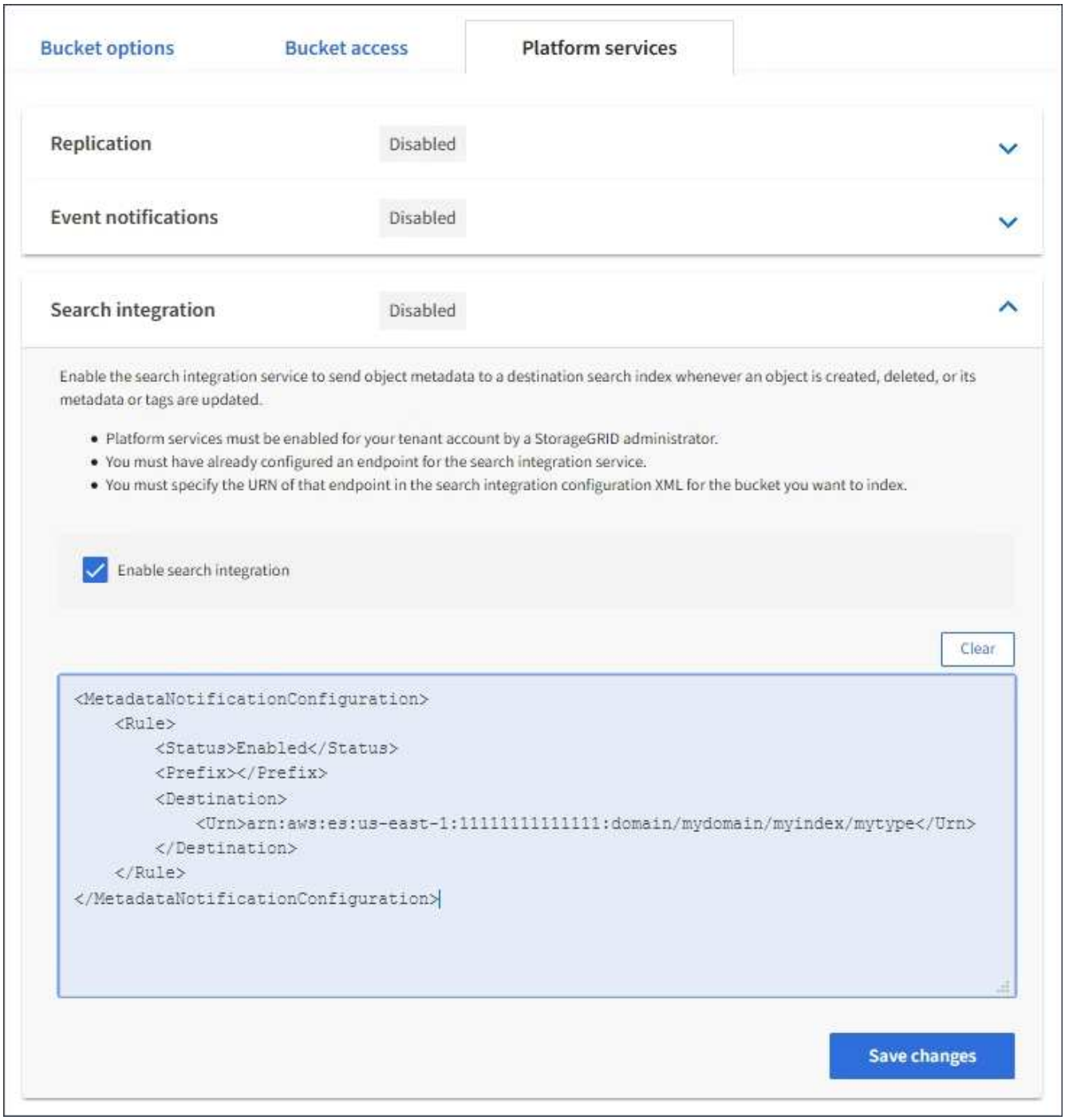
1. 使用文本编辑器创建启用搜索集成所需的元数据通知 XML 。
   - 请参见有关用于搜索集成的配置 XML 的信息。
   - 配置 XML 时，请使用搜索集成端点的 URN 作为目标。

```
<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 * 存储（ S3 ） * > * 分段 * ，然后取消选中 * 启用搜索集成 * 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"

"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，您无法在索引中编辑文档的字段类型。