配置平台服务端点

StorageGRID 11.8

NetApp
March 19, 2024

目录

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。对于单个租户、您最多可以配置500个平台服务端点。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。您还可以将源存储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：将有关对象创建的通知发送到一个Amazon Simple Notification Service (Amazon SNS)主题、将有关对象删除的通知发送到另一个Amazon SNS主题。

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Amazon SNS和Kafka端点。不支持简单队列服务(Simple Queue Service、SQS)或AWS Lamba端点。

对于Kafka端点、不支持相互TLS。因此、如果您有 `ssl.client.auth` 设置为 `required` 在Kafka代理配置中、可能会出现发生原因Kafka端点配置问题。

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` 或 `kafka`
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	`bucket-name`
通知	`sns-topic-name` 或 `kafka-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：

指定Amazon Simple Notification Service端点：

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

指定Kafka端点：

```
urn:mysite:kafka:optional:optional:kafka-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：Amazon Simple Notification Service (Amazon SNS)或Kafka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）：

AWS搜索集成端点

对于AWS搜索集成端点、您可以使用以下凭据：

- 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。

CloudMirror复制和**Amazon SNS**端点

对于CloudMirror复制和Amazon SNS端点、您可以使用以下凭据：

- 访问密钥：访问密钥 ID 和机密访问密钥
- 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。

Kafka端点

对于Kafka端点、您可以使用以下凭据：

- SASL/PLAIN：用户名和密码
- SASL/SCRAM-SHA-256：用户名和密码
- SASL/SCRAM-SHA-512：用户名和密码

  - 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、则会使用以下默认端口：

- 端口443用于HTTPS URL、端口80用于HTTP URL (大多数端点)
- 用于HTTPS和HTTP URI的端口9092 (仅限Kafka端点)

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。

AWS搜索集成端点

输入或上传AWS搜索集成端点的凭据。

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）

CloudMirror复制或**Amazon SNS**端点

输入或上传用于CloudMirror复制或Amazon SNS端点的凭据。

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

Authentication type	Description	凭据
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）

Kafka端点

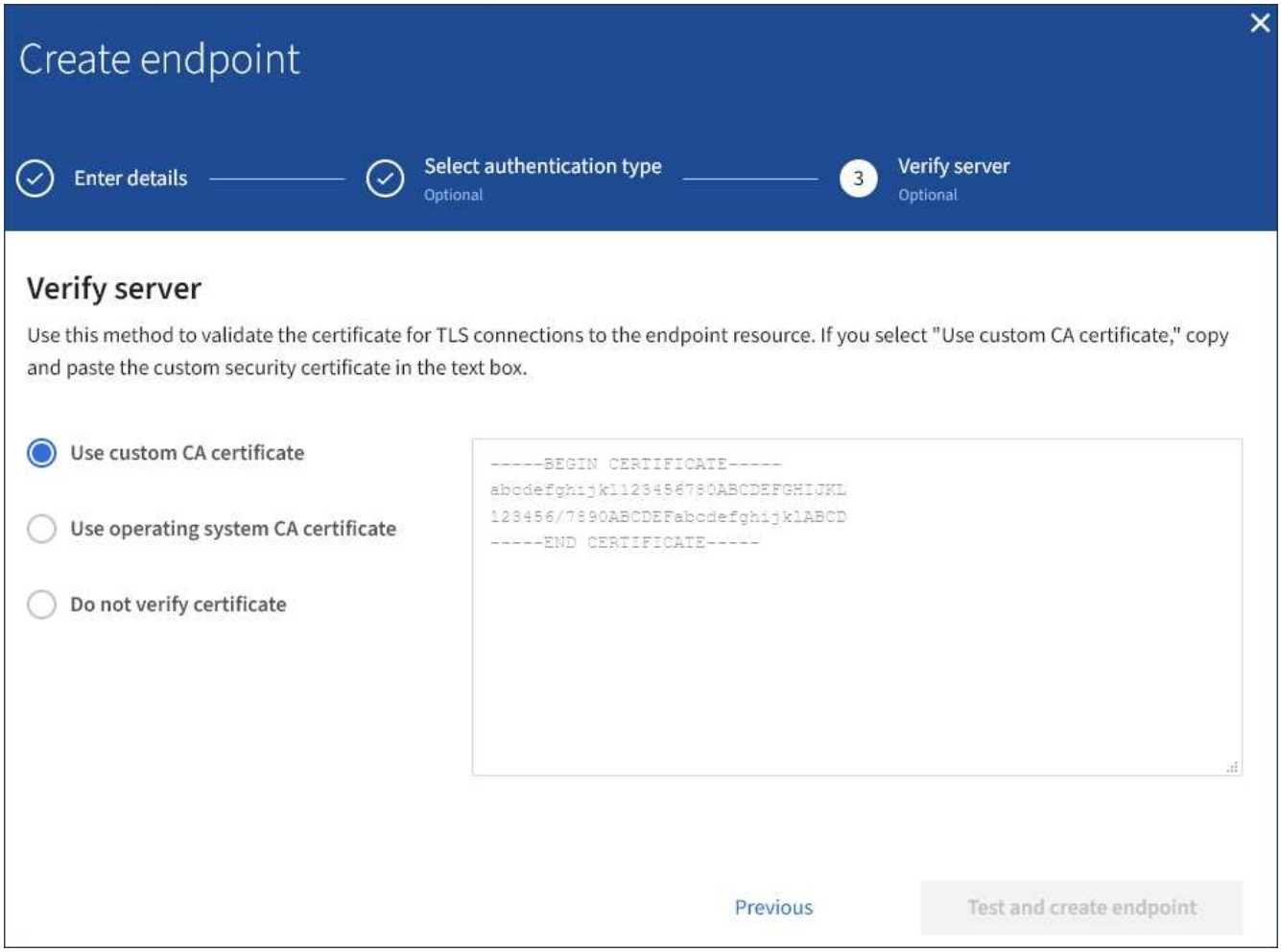
输入或上传Kafka端点的凭据。

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。
SASL/普通	使用带有纯文本的用户名和密码对目标连接进行身份验证。	• Username • Password
SASL/SCRAM-SHA-256	使用用户名和密码并使用质询响应协议和SHA-256哈希对目标连接进行身份验证。	• Username • Password
SASL/SCRAM-SHA-512	使用用户名和密码并使用质询响应协议和SHA-512哈希对目标连接进行身份验证。	• Username • Password

如果用户名和密码源自从Kafka集群获取的委派令牌，请选择*使用委派进行身份验证*。

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"。

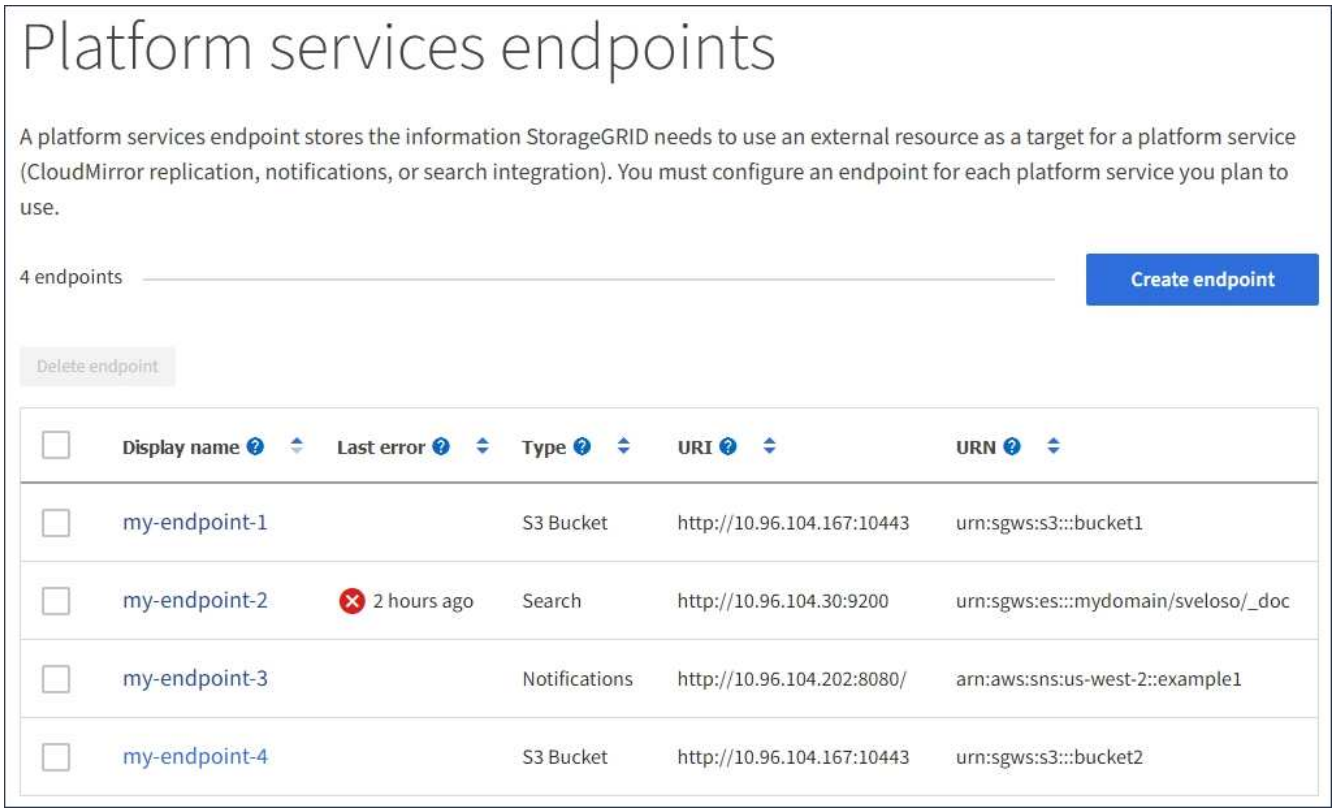
关于此任务

StorageGRID 不会验证这些凭据是否具有正确的权限。

步骤

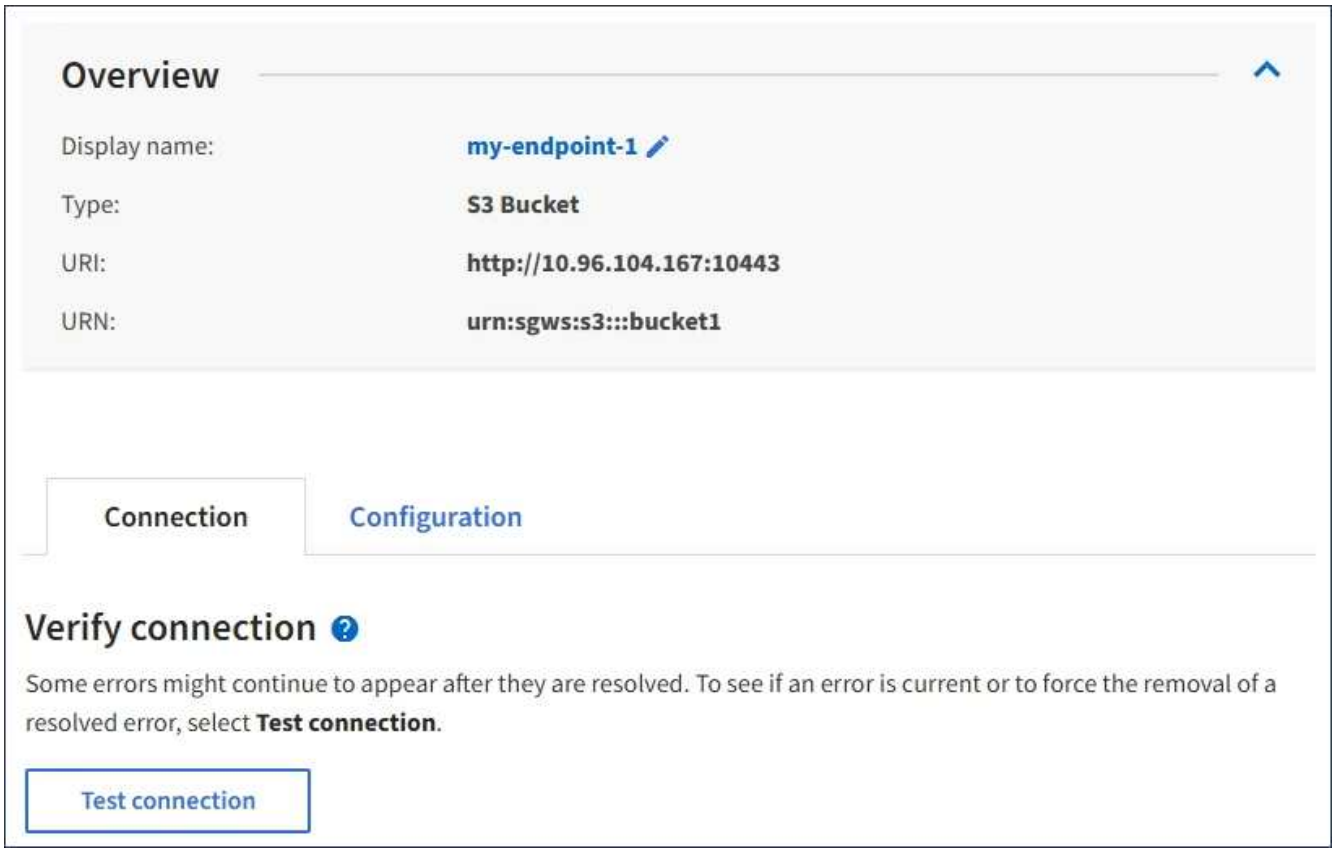
1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   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。

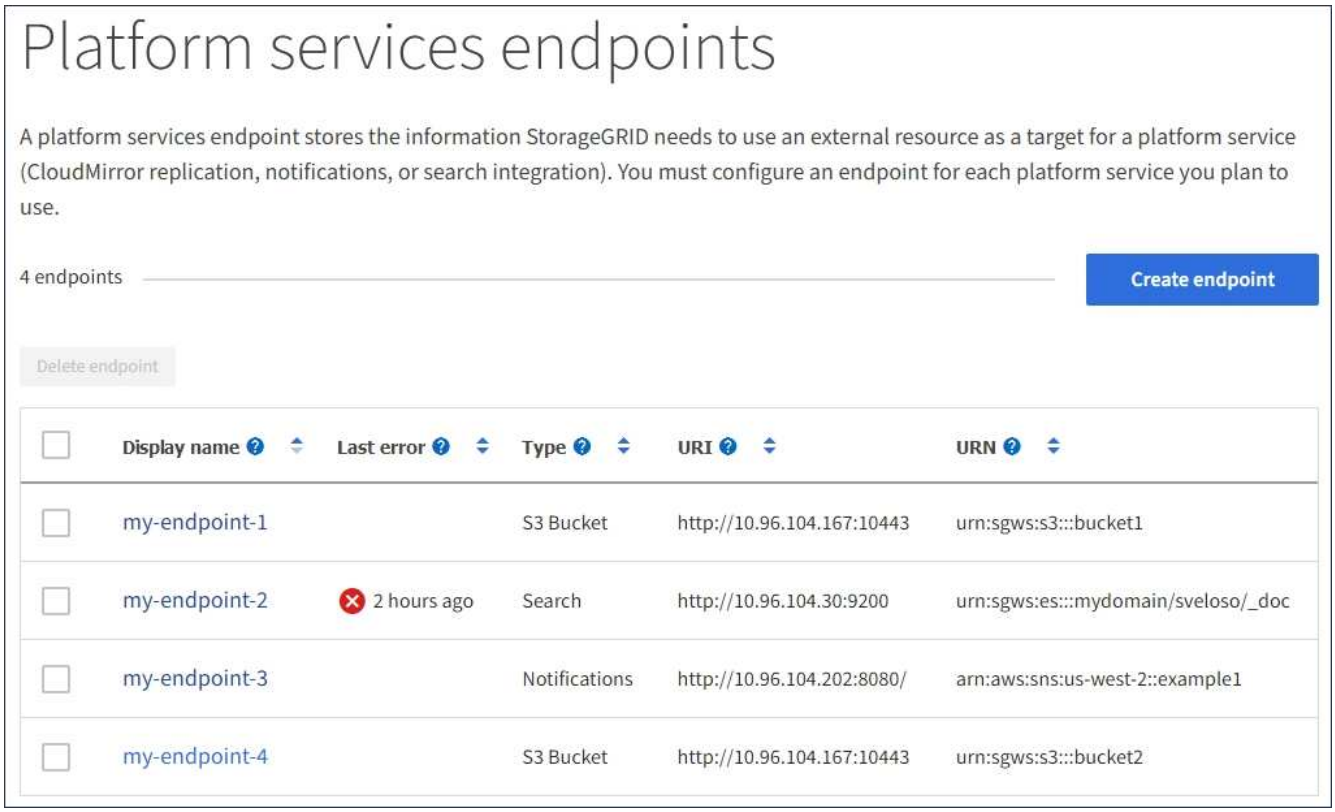
开始之前

- 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 * 。
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 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。

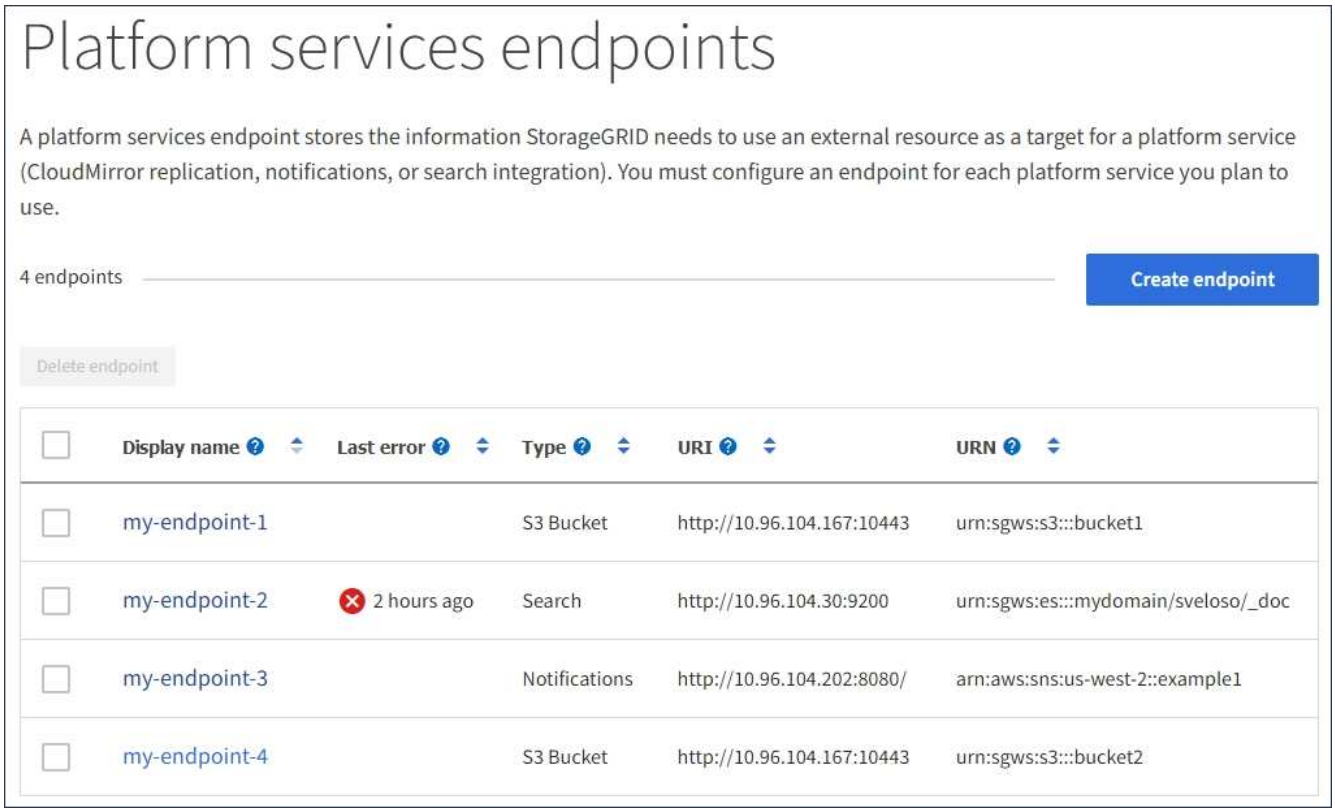
开始之前

- 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。

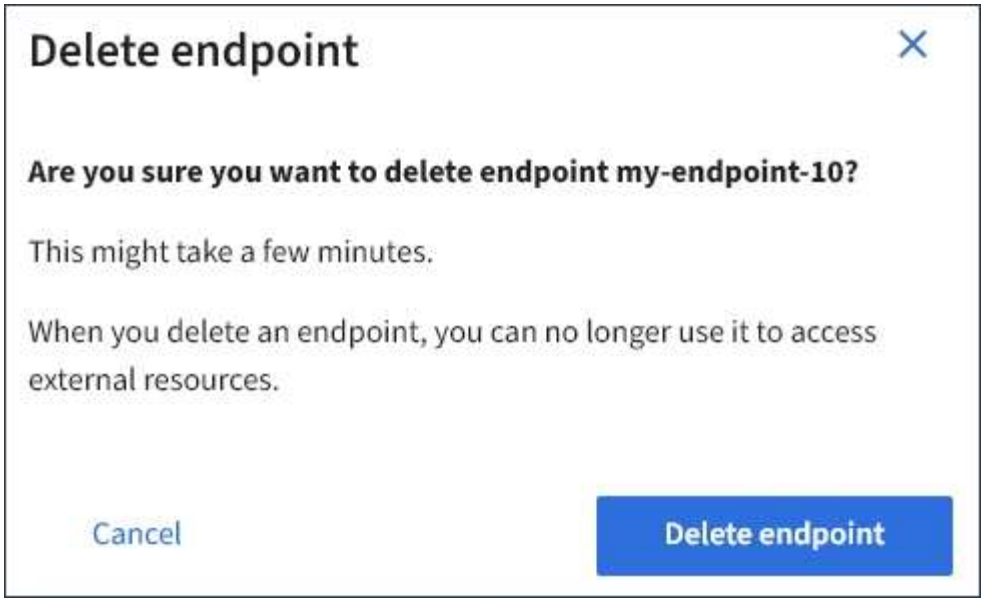


2. 选中要删除的每个端点对应的复选框。

   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。



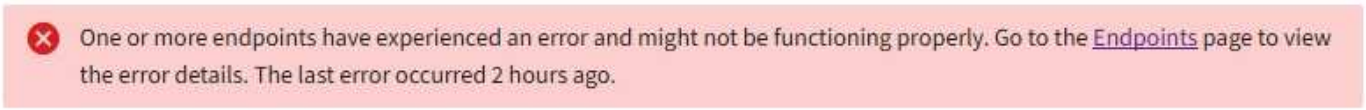
4. 选择 * 删除端点 * 。

解决平台服务端点错误

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

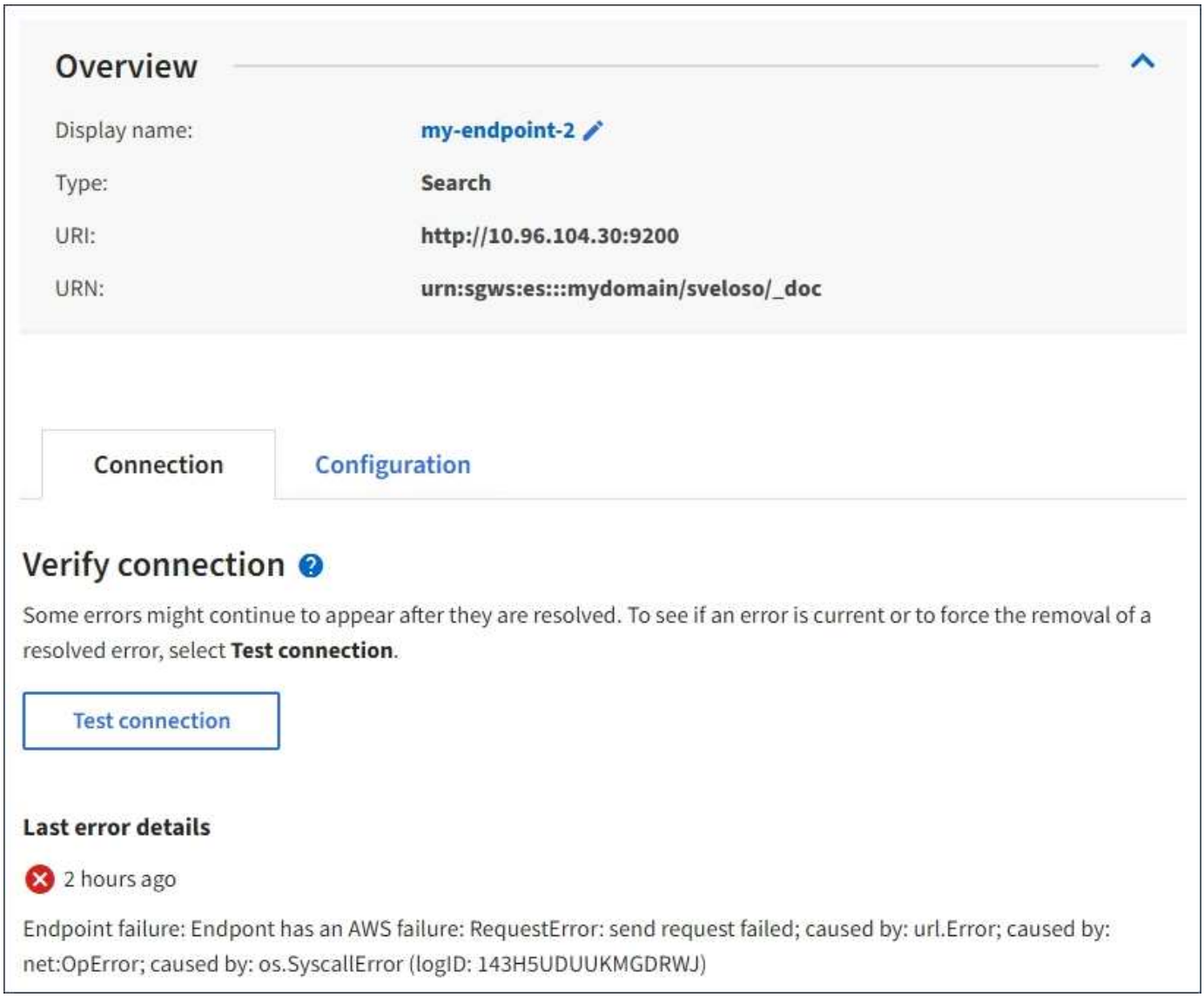
如果在过去7天内发生任何平台服务端点错误、租户管理器信息板将显示警报消息。您可以转到平台服务端点页面以查看有关此错误的更多详细信息。



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"端点凭据或目标访问需要更新"、详细信息为"AccessDenied"或"InvvalidAccessKeyId"。

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、如果在尝试使用平台服务时收到错误(例如"403禁止")、请检查与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"