控制管理员对StorageGRID 的访问

StorageGRID 11.5

NetApp
April 11, 2024

目录

控制管理员对StorageGRID 的访问

您可以通过以下方式控制管理员对StorageGRID 系统的访问：打开或关闭防火墙端口、管理管理组和用户、配置单点登录(Single Sign-On、SSO)以及提供客户端证书以允许对StorageGRID 指标进行安全外部访问。

- "通过防火墙控制访问"
- "使用身份联合"
- "管理管理组"
- "管理本地用户"
- "对StorageGRID 使用单点登录(SSO)"
- "配置管理员客户端证书"

通过防火墙控制访问

如果要通过防火墙控制访问，请打开或关闭外部防火墙上的特定端口。

在外部防火墙上控制访问

您可以通过在外部防火墙中打开或关闭特定端口来控制对 StorageGRID 管理节点上用户界面和 API 的访问。例如，除了使用其他方法控制系统访问之外，您可能还希望防止租户能够在防火墙处连接到网格管理器。

Port	Description	端口是否已打开 ...
443.	管理节点的默认 HTTPS 端口	Web 浏览器和管理 API 客户端可以访问网格管理器，网格管理 API ，租户管理器和租户管理 API 。 • 注： * 端口 443 也用于某些内部流量。
8443	管理节点上的网格管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问网格管理器和网格管理 API 。 • Web 浏览器和管理 API 客户端无法访问租户管理器或租户管理 API 。 • 请求内部内容将被拒绝。
9443	管理节点上的租户管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问租户管理器和租户管理 API 。 • Web 浏览器和管理 API 客户端无法访问网格管理器或网格管理 API 。 • 请求内部内容将被拒绝。

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。

相关信息

"登录到网格管理器"

"如果StorageGRID 未使用SSO、则创建租户帐户"

"摘要：客户端连接的 IP 地址和端口"

"管理不可信客户端网络"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"安装 Red Hat Enterprise Linux 或 CentOS"

使用身份联合

使用身份联合可以加快设置组和用户的速度，并允许用户使用熟悉的凭据登录到StorageGRID 。

配置身份联合

如果您希望在Active Directory、OpenLDAP或Oracle Directory Server等其他系统中管理管理管理组和用户、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网格管理器。
- 您必须具有特定的访问权限。
- 如果您计划启用单点登录(SSO)、则必须使用Active Directory作为联合身份源、并使用AD FS作为身份提供程序。请参见"`使用单点登录的要求。`"
- 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

如果要导入以下类型的联合组、则必须为网格管理器配置身份源：

- 管理组。管理组中的用户可以登录到网格管理器并根据分配给该组的管理权限执行任务。
- 不使用自己身份源的租户的租户用户组。租户组中的用户可以登录到租户管理器，并根据在租户管理器中为该组分配的权限执行任务。

步骤

1. 选择*配置*>*访问控制*>*身份联合*。

2. 选择 * 启用身份联合 * 。

   此时将显示用于配置LDAP服务器的字段。

3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。

   您可以选择* Active Directory*、* OpenLDAP*或*其他*。

   > 如果选择* OpenLDAP*、则必须配置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。

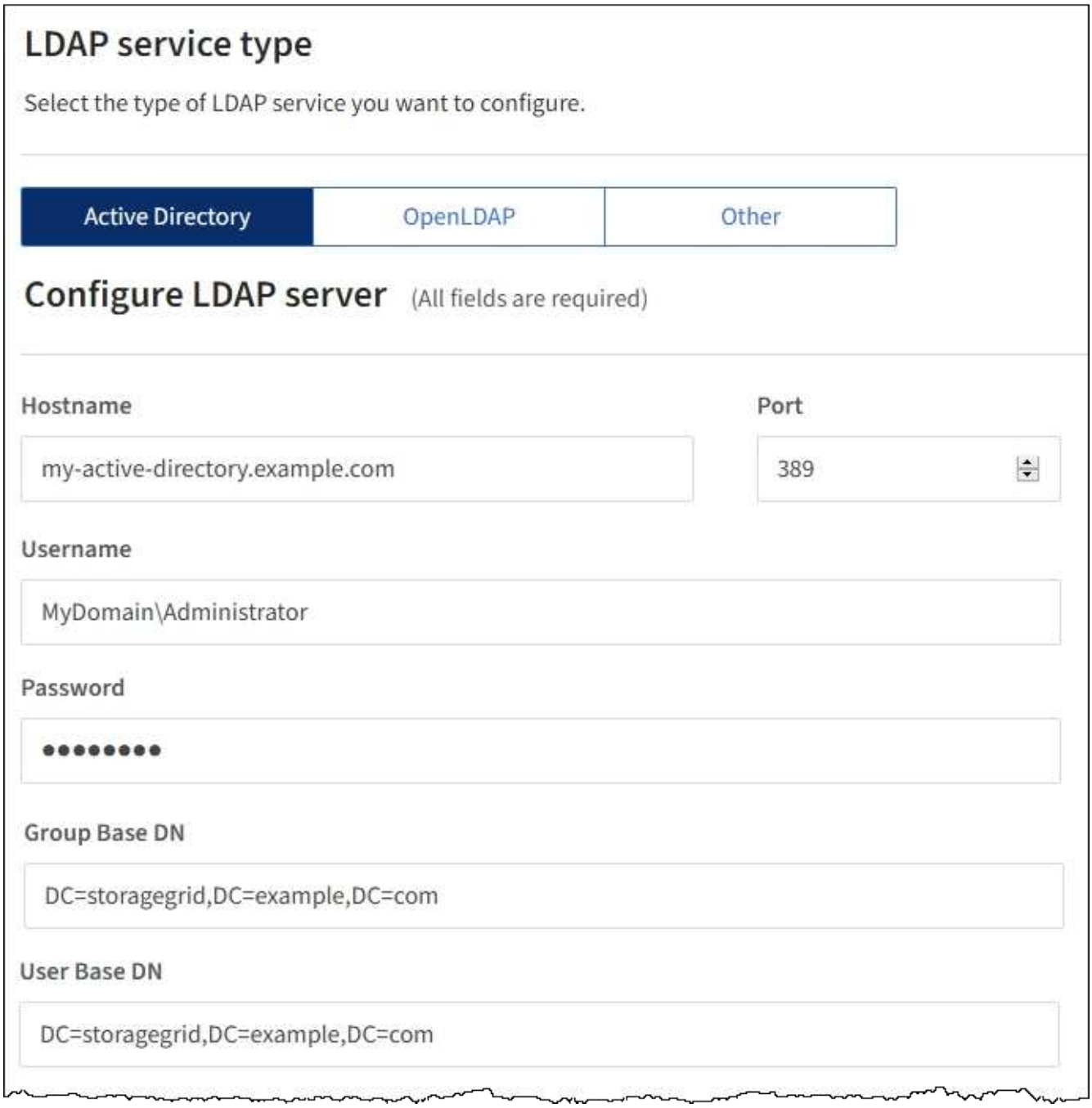
     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

8. 或者、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

"支持传出 TLS 连接的密码"

"使用单点登录的要求"

"创建租户帐户"

"使用租户帐户"

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。

相关信息

"OpenLDAP 文档：版本 2.4 管理员指南"

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网格管理器。
- 您必须具有特定的访问权限。
- 必须启用身份源。

步骤

1. 选择*配置*>*访问控制*>*身份联合*。

   此时将显示"Identity Federation"页面。*同步*按钮位于页面底部。

2. 单击*同步*。

   确认消息指示同步已成功启动。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。

正在禁用身份联合

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 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 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*已启用*或*沙盒模式*、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 * 。

步骤

1. 选择*配置*>*访问控制*>*身份联合*。
2. 取消选中*启用身份联合*复选框。
3. 单击 * 保存 * 。

相关信息

"禁用单点登录"

管理管理组

您可以创建管理组来管理一个或多个管理员用户的安全权限。用户必须属于要授予对 StorageGRID 系统访问权限的组。

创建管理组

通过管理组，您可以确定哪些用户可以访问网格管理器和网格管理 API 中的哪些功能和操作。

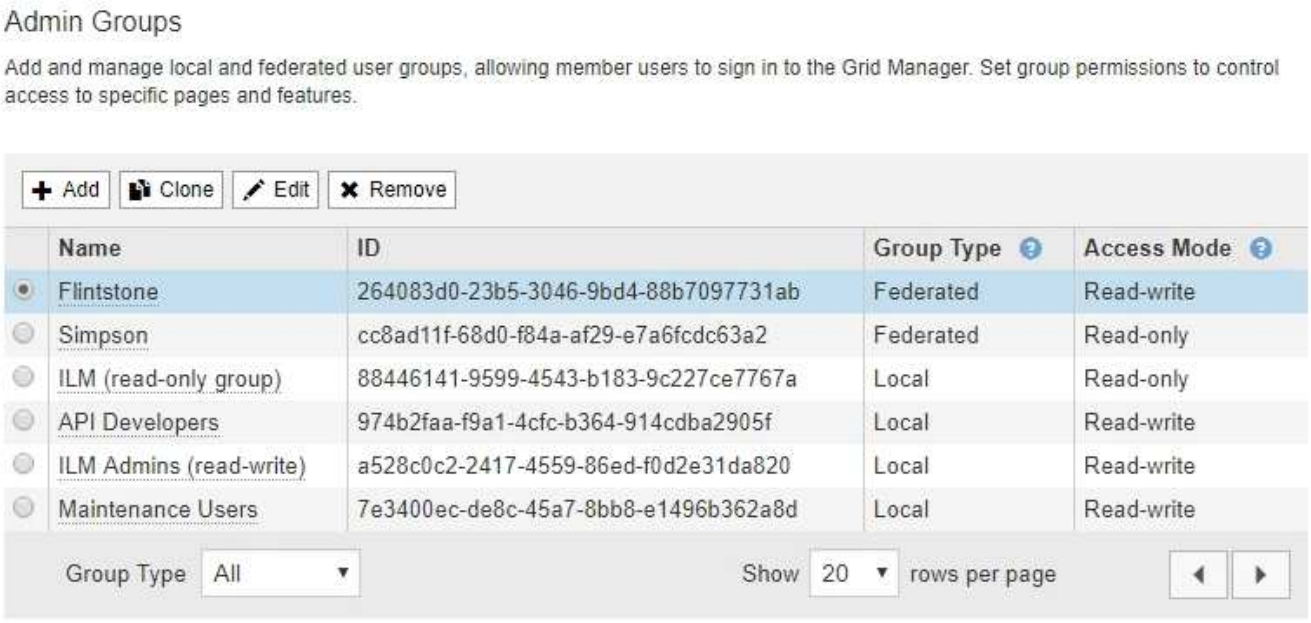
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 如果您计划导入联合组、则必须已配置身份联合、并且已配置的身份源中必须已存在此联合组。

步骤

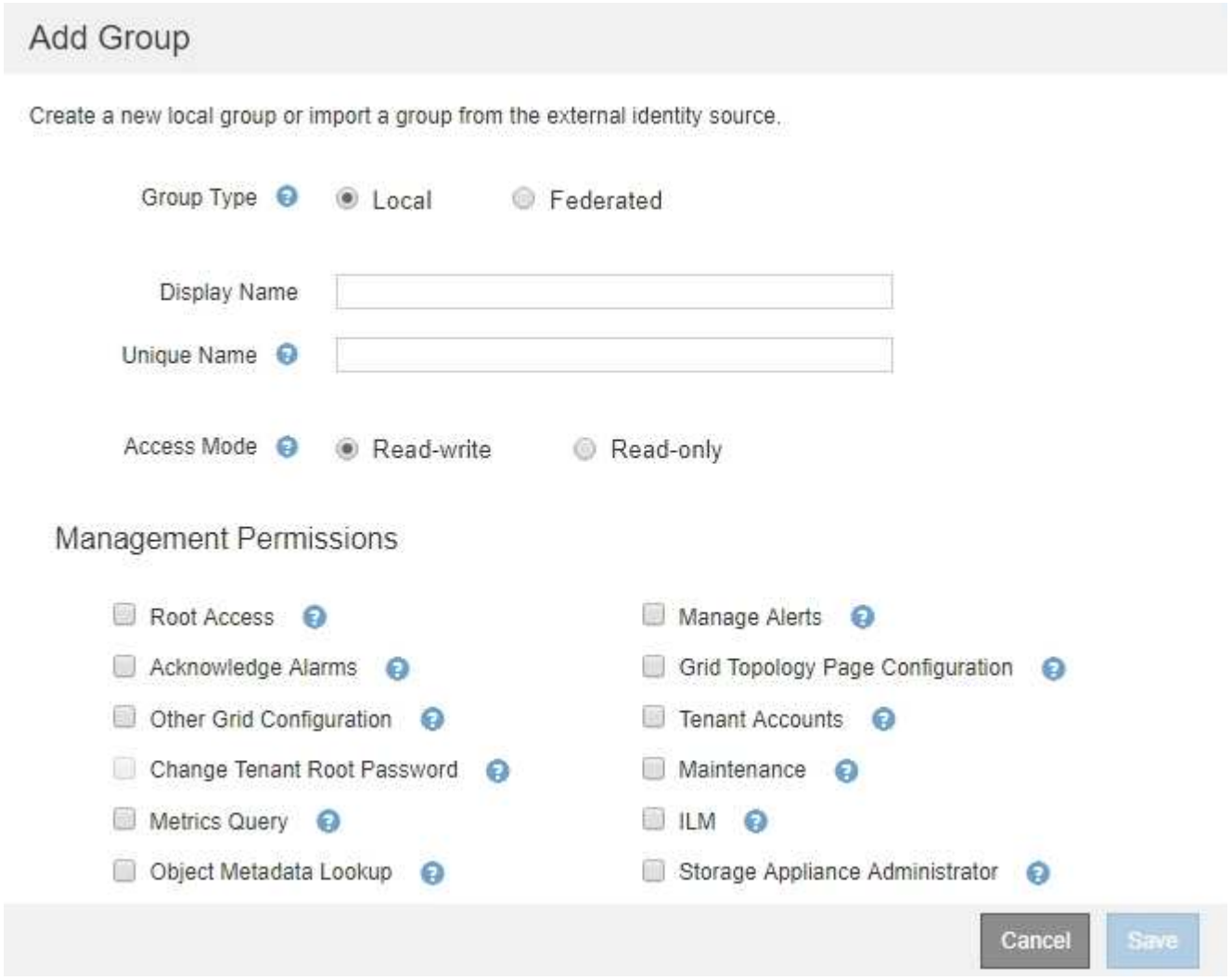
1. 选择*配置访问控制管理组。

   此时将显示Admin Groups页面、其中列出了任何现有的管理组。



2. 选择 * 添加 * 。

此时将显示添加组对话框。



3. 对于组类型、如果要创建仅在StorageGRID 中使用的组、请选择*本地*；如果要从身份源导入组、请选择*联合*。
4. 如果选择了*本地*、请输入组的显示名称。显示名称是显示在网格管理器中的名称。例如，" M维护用户 " 或 "`ILM 管理员。`
5. 输入组的唯一名称。
   - 本地：输入所需的唯一名称。例如、“ILM管理员。”
   - 联合：输入组在配置的身份源中显示的名称。
6. 对于*访问模式*、选择组中的用户是否可以在网格管理器和网格管理API中更改设置并执行操作、或者选择他们是否只能查看设置和功能。
   - * 读写 *（默认）：用户可以更改其管理权限允许的设置并执行这些操作。
   - * 只读 *：用户只能查看设置和功能。他们不能在网格管理器或网格管理 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。

7. 选择一个或多个管理权限。

   您必须为每个组至少分配一个权限；否则，属于该组的用户将无法登录到 StorageGRID 。
8. 选择 * 保存 * 。

   此时将创建新组。如果此组为本地组、则现在可以添加一个或多个用户。如果这是联合组、则身份源将管理属于该组的用户。

相关信息

"管理本地用户"

管理组权限

创建管理员用户组时，您可以选择一个或多个权限来控制对网格管理器特定功能的访问。然后，您可以将每个用户分配给一个或多个管理组，以确定用户可以执行的任务。

您必须为每个组至少分配一个权限；否则、属于该组的用户将无法登录到网格管理器。

默认情况下，属于至少具有一个权限的组的任何用户均可执行以下任务：

- 登录到网格管理器
- 查看信息板
- 查看节点页面
- 监控网格拓扑
- 查看当前警报和已解决警报
- 查看当前和历史警报（旧系统）
- 更改自己的密码（仅限本地用户）

- 在配置和维护页面上查看特定信息

以下各节介绍了在创建或编辑管理组时可以分配的权限。未明确提及的任何功能都需要root访问权限。

根访问

通过此权限，可以访问所有网格管理功能。

管理警报

通过此权限，您可以访问用于管理警报的选项。用户必须具有此权限才能管理静音，警报通知和警报规则。

确认警报(旧系统)

此权限可用于确认和响应警报（旧系统）。所有已登录用户均可查看当前和历史警报。

如果您希望用户仅监控网格拓扑并确认警报，则应分配此权限。

网格拓扑页面配置

通过此权限、您可以访问以下菜单选项：

- 可从*支持*工具网格拓扑*页面访问的配置选项卡。
- 节点***事件*选项卡上的*重置事件计数*链接。

其他网格配置

通过此权限可以访问其他网格配置选项。

要查看这些附加选项、用户还必须具有网格拓扑页面配置权限。

- 警报(旧系统)：
  - 全局警报
  - 旧电子邮件设置
- * ILM ：
  - 存储池
  - 存储等级
- 配置*网络设置
  - 链路成本
- 配置*系统设置：
  - 显示选项
  - 网格选项
  - 存储选项
- 配置*监控*：

- 事件
- 支持：
  - AutoSupport

租户帐户

通过此权限可以访问*租户***租户帐户*页面。

网格管理API版本1 (已弃用)使用此权限管理租户组策略、重置Swift管理员密码以及管理root用户S3访问密钥。

更改租户**root**密码

通过此权限、您可以访问租户帐户页面上的*更改根密码*选项、从而可以控制谁可以更改租户的本地root用户的密码。不具有此权限的用户无法看到*更改根密码*选项。

您必须先为组分配租户帐户权限、然后才能分配此权限。

维护

通过此权限、您可以访问以下菜单选项：

- 配置*系统设置：
  - 域名*
  - 服务器证书*
- 配置*监控*：
  - 审核*
- 配置*访问控制：
  - 网格密码
- 维护*维护任务*
  - 停用
  - 扩展
  - 恢复
- 维护*网络：
  - DNS服务器*
  - 网格网络*
  - NTP服务器*
- 维护*系统：
  - 许可证*
  - 恢复软件包

- 软件更新
- 支持*工具：
  - 日志
- 没有维护权限的用户可以查看但不能编辑标有星号的页面。

指标查询

通过此权限、您可以访问*支持*工具*指标*页面。通过此权限，还可以使用网格管理 API 的 * 指标 * 部分访问自定义的 Prometheus 指标查询。

ILM

通过此权限，您可以访问以下 * ILM * 菜单选项：

- 擦除编码
- 规则
- * 策略 *
- 区域

> 对* ILM *存储池*和 ILM *存储级别*菜单选项的访问由"其他网格配置"和"网格拓扑页面配置"权限控制。

对象元数据查找

通过此权限可以访问* ILM *对象元数据查找*菜单选项。

存储设备管理员

通过此权限，您可以通过网格管理器访问存储设备上的 E 系列 SANtricity 系统管理器。

权限与访问模式之间的交互

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。

从网格管理**API**停用功能

您可以使用网格管理 API 完全停用 StorageGRID 系统中的某些功能。停用某个功能后，不能为任何人分配执行与该功能相关的任务的权限。

关于此任务

停用的功能系统允许您阻止访问 StorageGRID 系统中的某些功能。停用某个功能是防止root用户或具有root访问权限的管理组中的用户能够使用该功能的唯一方法。

要了解此功能的有用程度，请考虑以下情形：

_Company A 是一家服务提供商，通过创建租户帐户租用其 StorageGRID 系统的存储容量。为了保护租户对象的安全， A 公司希望确保自己的员工在部署帐户后永远不能访问任何租户帐户。 _

_Company A 可以通过使用网格管理 API 中的停用功能系统来实现此目标。通过完全停用网格管理器中的*更改租户根密码*功能(UI和API)、公司A可以确保任何管理员用户(包括root用户和具有root访问权限的组中的用户)都不能更改任何租户帐户的root用户的密码

重新激活已停用的功能

默认情况下，您可以使用网格管理 API 重新激活已停用的功能。但是，如果要防止重新激活已停用的功能，则可以停用 * 激活功能 * 功能本身。

> 无法重新激活 * 活动功能 * 功能。如果您决定停用此功能，请注意，您将永远无法重新激活任何其他已停用的功能。要还原任何丢失的功能，您必须联系技术支持。

有关详细信息、请参见实施S3或Swift客户端应用程序的说明。

步骤

1. 访问网格管理 API 的 Swagger 文档。
2. 找到停用功能端点。
3. 要停用*更改租户根密码*等功能、请向API发送如下正文：

```
{ "grid": {"changeTenantRootPassword": true} }
```

请求完成后、更改租户根密码功能将被禁用。用户界面中不再显示更改租户根密码管理权限、尝试更改租户根密码的任何API请求将失败、并显示"`403 For禁用。`

4. 要重新激活所有功能，请按如下所示将正文发送到 API ：

```
{ "grid": null }
```

此请求完成后、包括更改租户root密码功能在内的所有功能都将重新激活。此时、"更改租户根密码"管理权限将显示在用户界面中、如果用户拥有" root访问"或"更改租户根密码"管理权限、则尝试更改租户根密码的任何API请求都将成功。

> 上一示例将重新激活 *all* 已停用的功能。如果其他功能已停用，而这些功能应保持停用状态，则必须在 PUT 请求中明确指定它们。例如、要重新激活更改租户root密码功能并继续停用警报确认功能、请发送此PUT请求：

```
{ "grid": { "alarmAcknowledgment": true } }
```

相关信息

"使用网格管理API"

修改管理组

您可以修改管理组以更改与该组关联的权限。对于本地管理组、您还可以更新显示名称。

您需要的内容

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

步骤

1. 选择*配置访问控制管理组。
2. 选择组。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 单击 * 编辑 * 。
4. M、对于本地组、输入将显示给用户的组名称、例如"维护用户"。

   您不能更改唯一名称、即内部组名称。

5. 也可以更改组的访问模式。
   - * 读写 * （默认）： 用户可以更改其管理权限允许的设置并执行这些操作。
   - * 只读 * ： 用户只能查看设置和功能。他们不能在网格管理器或网格管理 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。

6. 也可以添加或删除组权限。

   请参见有关管理组权限的信息。

7. 选择 * 保存 * 。

相关信息

[管理组权限]

删除管理组

如果要从系统中删除某个管理组，则可以删除该组，并删除与该组关联的所有权限。删除管理员组会从该组中删除任何管理员用户、但不会删除这些管理员用户。

您需要的内容

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

关于此任务

删除组时、分配给该组的用户将丢失对网格管理器的所有访问权限、除非其他组授予了这些用户的权限。

步骤

1. 选择*配置访问控制管理组。
2. 选择组的名称。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 选择 * 删除 * 。
4. 选择 * 确定 * 。

管理本地用户

您可以创建本地用户并将其分配给本地管理组、以确定这些用户可以访问哪些网格管理器功能。

网格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。

如果已启用单点登录(SSO)、则本地用户无法登录到StorageGRID。

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

创建本地用户

如果已创建本地管理组、则可以创建一个或多个本地用户、并将每个用户分配给一个或多个组。组的权限控制用户可以访问的网格管理器功能。

关于此任务

您只能创建本地用户、并且只能将这些用户分配给本地管理组。联合用户和联合组使用外部身份源进行管理。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 单击 * 创建 * 。
3. 输入用户的显示名称、唯一名称和密码。
4. 将用户分配给一个或多个控制访问权限的组。

   组名称列表是从组表生成的。

5. 单击 * 保存 * 。

相关信息

"管理管理组"

修改本地用户的帐户

您可以修改本地管理员用户的帐户以更新用户的显示名称或组成员资格。您还可以临时阻止用户访问系统。

关于此任务

您只能编辑本地用户。联合用户详细信息会自动与外部身份源同步。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 选择要编辑的用户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 单击 * 编辑 * 。
4. 或者、也可以更改名称或组成员资格。
5. 或者、要防止用户临时访问系统、请选中*拒绝访问*。
6. 单击 * 保存 * 。

   新设置将在用户下次注销后重新登录到网格管理器时应用。

删除本地用户的帐户

您可以删除不再需要访问网格管理器的本地用户帐户。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 选择要删除的本地用户。

   您不能删除预定义的root本地用户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 单击 * 删除 * 。
4. 单击 * 确定 * 。

更改本地用户的密码

本地用户可以使用网格管理器横幅中的 * 更改密码 * 选项更改自己的密码。此外、有权访问Admin Users页面的用户还可以更改其他本地用户的密码。

关于此任务

您只能更改本地用户的密码。联合用户必须在外部身份源中更改自己的密码。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 从用户页面中、选择用户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器

的"查找"功能在当前显示的行中搜索特定项。

3. 单击*更改密码*。
4. 输入并确认密码、然后单击*保存*。

对StorageGRID 使用单点登录(SSO)

StorageGRID 系统支持使用安全断言标记语言 2.0 （ SAML 2.0 ）标准的单点登录（ SSO ）。启用 SSO 后，所有用户都必须经过外部身份提供程序的身份验证，然后才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。本地用户无法登录到 StorageGRID 。

- "单点登录的工作原理"
- "使用单点登录的要求"
- "配置单点登录"

单点登录的工作原理

在启用单点登录（ SSO ）之前，请查看启用 SSO 后 StorageGRID 登录和注销过程会受到什么影响。

启用SSO后登录

启用 SSO 并登录到 StorageGRID 后，系统会将您重定向到组织的 SSO 页面以验证您的凭据。

步骤

1. 在 Web 浏览器中输入任何 StorageGRID 管理节点的完全限定域名或 IP 地址。

   此时将显示 StorageGRID 登录页面。

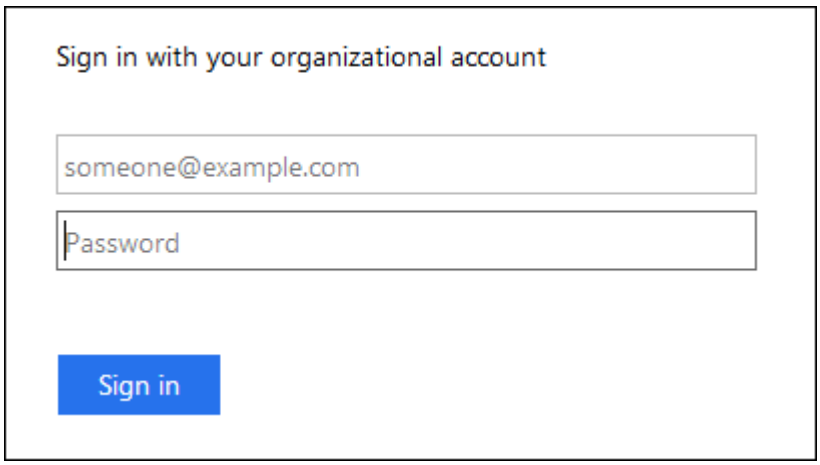
   - 如果这是您首次在此浏览器上访问此 URL ，系统将提示您输入帐户 ID ：

   - 如果您之前访问过网格管理器或租户管理器，系统将提示您选择最近的帐户或输入帐户 ID ：

输入租户帐户的完整URL (即、完全限定域名或IP地址后跟)时、不会显示StorageGRID 登录页面 `/?accountId=20-digit-account-id`）。而是会立即重定向到您所在组织的 SSO 登录页面，您可以在该页面上进行登录 使用您的 SSO 凭据登录。

2. 指示您是要访问网格管理器还是租户管理器：
   - 要访问网格管理器、请将"帐户**ID**"*字段留空、输入 0 作为帐户**ID**、或者如果"*网格管理器"显示在近期帐户列表中、请选择此选项。
   - 要访问租户管理器，请输入 20 位租户帐户 ID ，或者如果某个租户显示在近期帐户列表中，则按名称选择此租户。
3. 单击*登录*

   StorageGRID 会将您重定向到贵组织的 SSO 登录页面。例如：



4. 【签名 _sso]] 使用您的 SSO 凭据登录。

   如果您的 SSO 凭据正确：

   a. 身份提供程序（ IdP ）为 StorageGRID 提供身份验证响应。
   b. StorageGRID 将验证身份验证响应。
   c. 如果响应有效、并且您属于具有足够访问权限的联合组、则您将登录到网格管理器或租户管理器、具体取决于您选择的帐户。

5. 或者，如果您拥有足够的权限，也可以访问其他管理节点，或者访问网格管理器或租户管理器。

   您无需重新输入 SSO 凭据。

启用SSO后注销

为 StorageGRID 启用 SSO 后，注销时会发生什么情况取决于您登录到的内容以及注销的位置。

步骤

1. 找到用户界面右上角的 * 注销 * 链接。
2. 单击*注销*。

   此时将显示 StorageGRID 登录页面。更新了 * 近期帐户 * 下拉列表，其中包含 * 网格管理器 * 或租户名称，以便您将来可以更快地访问这些用户界面。

如果您已登录到 ...	您可以从以下位置注销 ...	您已注销 ...
一个或多个管理节点上的网格管理器	任何管理节点上的网格管理器	所有管理节点上的网格管理器
一个或多个管理节点上的租户管理器	任何管理节点上的租户管理器	所有管理节点上的租户管理器
网格管理器和租户管理器	网格管理器	仅限网格管理器。您还必须注销租户管理器才能注销 SSO 。

下表总结了在使用单个浏览器会话时注销时会发生的情况。如果您通过多个浏览器会话登录到 StorageGRID ，则必须单独注销所有浏览器会话。

使用单点登录的要求

在为 StorageGRID 系统启用单点登录（ SSO ）之前，请查看本节中的要求。

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。

身份提供程序要求

用于SSO的身份提供程序(IdP)必须满足以下要求：

- 以下任一版本的Active Directory联合身份验证服务(AD FS)：
  - AD FS 4.0、随Windows Server 2016提供

    Windows Server 2016 应使用 "KB3201845 更新"或更高版本。

  - AD FS 3.0 ，随 Windows Server 2012 R2 更新或更高版本提供。

- 传输层安全（ Transport Layer Security ， TLS ） 1.2 或 1.3
- Microsoft .NET Framework 3.5.1 或更高版本

服务器证书要求

StorageGRID 在每个管理节点上使用管理接口服务器证书来保护对网格管理器、租户管理器、网格管理API和租户管理API的访问。在AD FS中为StorageGRID 配置SSO依赖方信任时、您可以使用服务器证书作为向AD FS发出StorageGRID 请求的签名证书。

如果尚未为管理接口安装自定义服务器证书、应立即安装。安装自定义服务器证书时、该证书将用于所有管理节点、您可以在所有StorageGRID 依赖方信任关系中使用该证书。

> 建议不要在AD FS依赖方信任关系中使用管理节点的默认服务器证书。如果节点发生故障而您恢复了该节点，则会生成一个新的默认服务器证书。在登录到已恢复的节点之前、您必须使用新证书更新AD FS中的依赖方信任。

您可以通过登录到管理节点的命令Shell并转到来访问管理节点的服务器证书 `/var/local/mgmt-api` 目录。自定义服务器证书名为 `custom-server.crt`。节点的默认服务器证书名为 `server.crt`。

相关信息

"通过防火墙控制访问"

"为网格管理器和租户管理器配置自定义服务器证书"

配置单点登录

启用单点登录（ SSO ）后，只有在用户凭据通过贵组织实施的 SSO 登录过程获得授权的情况下，用户才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。

- "确认联合用户可以登录"
- "使用沙盒模式"
- "在AD FS中创建依赖方信任"
- "测试依赖方信任"
- "启用单点登录"
- "禁用单点登录"
- "临时禁用并重新启用一个管理节点的单点登录"

确认联合用户可以登录

在启用单点登录（ SSO ）之前，您必须确认至少有一个联合用户可以登录到网格管理器以及任何现有租户帐户的租户管理器。

您需要的内容

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

- 您正在使用Active Directory作为联合身份源、使用AD FS作为身份提供程序。

  "使用单点登录的要求"

步骤

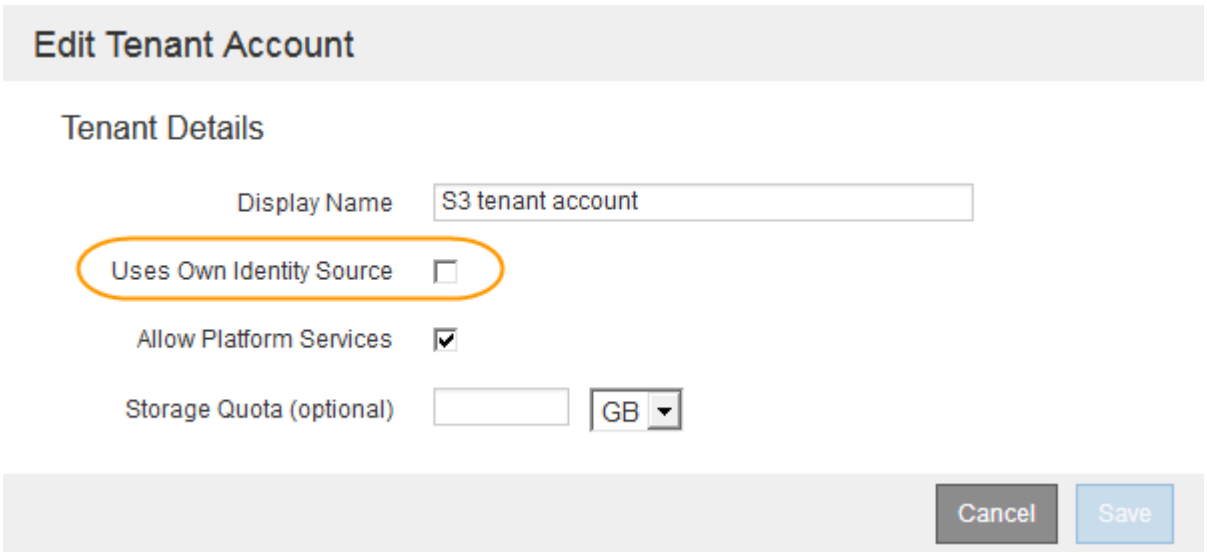
1. 如果存在现有租户帐户，请确认所有租户均未使用其自己的身份源。

   启用 SSO 后，在租户管理器中配置的身份源将被网格管理器中配置的身份源覆盖。属于租户身份源的用户将无法再登录，除非他们拥有网格管理器身份源帐户。

   a. 登录到每个租户帐户的租户管理器。
   b. 选择*访问控制*>*身份联合*。
   c. 确认未选中*启用身份联合*复选框。
   d. 如果是、请确认不再需要可能用于此租户帐户的任何联合组、取消选中此复选框、然后单击*保存*。

2. 确认联合用户可以访问网格管理器：
   a. 在网格管理器中、选择*配置*>*访问控制*>*管理组*。
   b. 确保已从Active Directory身份源导入至少一个联合组、并已为其分配"根访问"权限。
   c. 注销。
   d. 确认您可以以联合组中的用户身份重新登录到网格管理器。

3. 如果存在现有租户帐户、请确认具有root访问权限的联合用户可以登录：
   a. 在网格管理器中、选择*租户*。
   b. 选择租户帐户、然后单击*编辑帐户*。
   c. 如果选中了*使用自己的身份源*复选框、请取消选中该复选框、然后单击*保存*。



   此时将显示租户帐户页面。

   a. 选择租户帐户、单击*登录*、然后以本地root用户身份登录到租户帐户。

b. 在租户管理器中、单击*访问控制*>*组*。

c. 确保至少已为此租户为网格管理器中的一个联合组分配"根访问"权限。

d. 注销。

e. 确认您可以以联盟组中的用户身份重新登录到租户。

相关信息

"使用单点登录的要求"

"管理管理组"

"使用租户帐户"

使用沙盒模式

在为StorageGRID 用户强制实施单点登录(SSO)之前、您可以使用沙盒模式配置和测试依赖方信任的Active Directory联合身份验证服务(AD FS)。启用SSO后、您可以重新启用沙盒模式以配置或测试新的和现有的依赖方信任。重新启用沙盒模式会暂时禁用StorageGRID 用户的SSO。

您需要的内容

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

关于此任务

启用SSO后、如果用户尝试登录到管理节点、则StorageGRID 会向AD FS发送身份验证请求。反过来、AD FS会向StorageGRID 发送身份验证响应、指示授权请求是否成功。对于成功的请求、响应会为用户提供一个通用唯一标识符(UUID)。

要允许StorageGRID (服务提供商)和AD FS (身份提供程序)就用户身份验证请求进行安全通信、您必须在StorageGRID 中配置某些设置。接下来、您必须使用AD FS为每个管理节点创建依赖方信任。最后，您必须返回到 StorageGRID 以启用 SSO 。

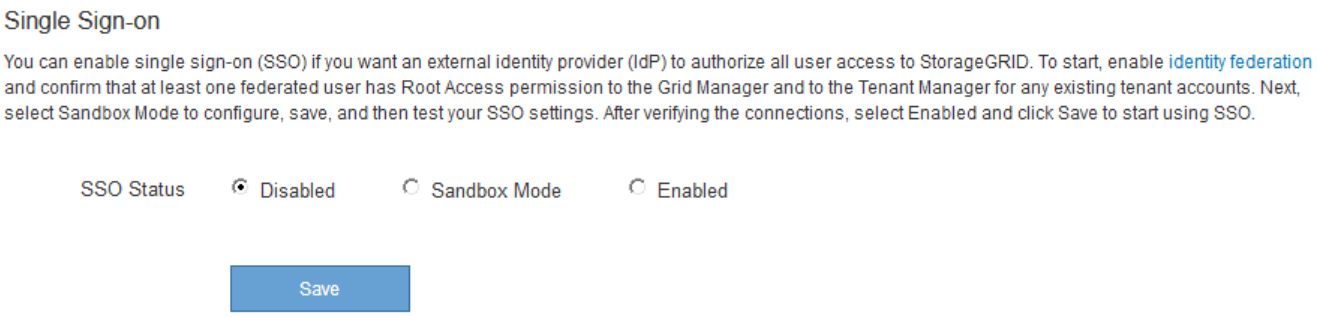
使用沙盒模式，可以轻松执行此背面配置，并在启用 SSO 之前测试所有设置。

强烈建议使用沙盒模式、但严格地说、这并不是必需的。如果您准备在StorageGRID 中配置SSO后立即创建AD FS依赖方信任、您无需测试每个管理节点的SSO和单点注销(SLO)进程、单击*已启用*、输入StorageGRID 设置、为AD FS中的每个管理节点创建依赖方信任、然后单击*保存*以启用SSO。

步骤

1. 选择*配置访问控制单点登录*。

   此时将显示 Single Sign-On 页面，并选择 * 已禁用 * 选项。



如果未显示SSO状态选项、请确认您已将Active Directory配置为联合身份源。请参见"`使用单点登录的要求。`"

2. 选择*沙盒模式*选项。

   此时将显示身份提供程序和依赖方设置。在身份提供程序部分中、*服务类型*字段为只读。它显示了您正在使用的身份联合服务的类型(例如Active Directory)。

3. 在身份提供程序部分中：

   a. 输入与AD FS中显示的名称完全相同的联合服务名称。

      要查找联合服务名称、请转到Windows Server Manager。选择*工具** AD FS管理*。从操作菜单中，选择 * 编辑联合身份验证服务属性 * 。联合服务名称显示在第二个字段中。

   b. 指定在身份提供程序响应StorageGRID 请求发送SSO配置信息时是否要使用传输层安全(TLS)来保护连接。

      - * 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 CA 证书确保连接安全。

        如果选择此设置、请在* CA证书*文本框中复制并粘贴此证书。

      - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。

4. 在依赖方部分中、指定在配置依赖方信任时要用于StorageGRID 管理节点的依赖方标识符。

   - 例如、如果您的网格只有一个管理节点、并且您预计将来不会添加更多管理节点、请输入 `SG` 或 `StorageGRID`。
   - 如果网格包含多个管理节点、请包含字符串 `[HOSTNAME]` 在标识符中。例如： `SG-[HOSTNAME]`。此操作将生成一个表、其中包含每个管理节点的依赖方标识符、该标识符基于节点的主机名。+注意：您必须为StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

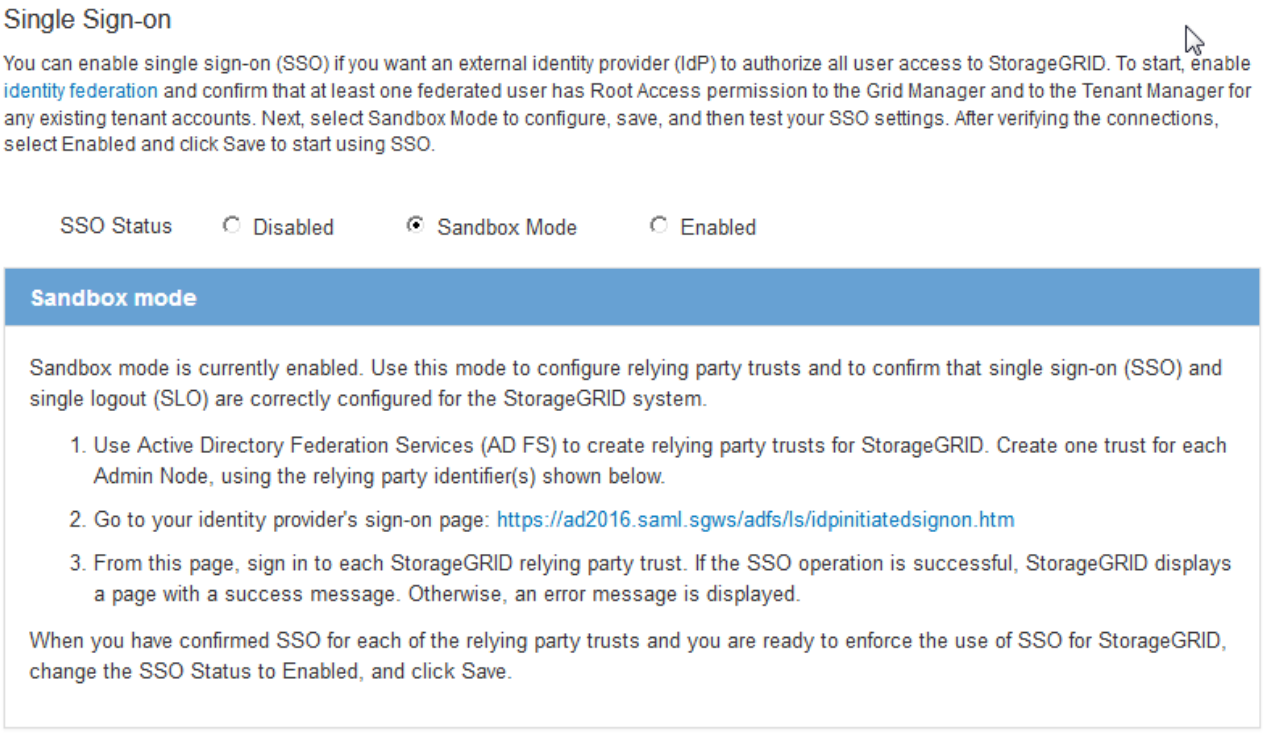
5. 单击 * 保存 * 。

   - 绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

   - 此时将显示沙盒模式确认通知、确认现在已启用沙盒模式。您可以在使用AD FS为每个管理节点配置依

赖方信任并测试单点登录(SSO)和单点注销(SLO)进程时使用此模式。



相关信息

"使用单点登录的要求"

在**AD FS**中创建依赖方信任

您必须使用 Active Directory 联合身份验证服务（ AD FS ）为系统中的每个管理节点创建依赖方信任。您可以使用 PowerShell 命令，从 StorageGRID 导入 SAML 元数据或手动输入数据来创建依赖方信任。

使用**Windows PowerShell**创建依赖方信任

您可以使用 Windows PowerShell 快速创建一个或多个依赖方信任。

您需要的内容

- 您已在StorageGRID 中配置SSO、并且知道系统中每个管理节点的完全限定域名(或IP地址)和依赖方标识符。

> 您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

- 您有在 AD FS 中创建依赖方信任的经验，也可以访问 Microsoft AD FS 文档。
- 您正在使用 AD FS 管理单元，并且属于管理员组。

关于此任务

这些说明适用于Windows Server 2016附带的AD FS 4.0。如果您使用的是Windows 2012 R2附带的AD FS 3.0、则会注意到操作步骤 略有不同。如果您有任何疑问，请参见 Microsoft AD FS 文档。

步骤

1. 从Windows开始菜单中、右键单击PowerShell图标、然后选择*以管理员身份运行*。
2. 在 PowerShell 命令提示符处，输入以下命令：

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - 适用于 `Admin_Node_Identifier`下、输入管理节点的依赖方标识符、与单点登录页面上显示的完全相同。例如： `SG-DC1-ADM1`。
   - 适用于 `Admin_Node_FQDN`下、输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）
3. 在 Windows Server Manager 中，选择 * 工具 * > * AD FS 管理 * 。

   此时将显示 AD FS 管理工具。
4. 选择 * AD FS* > * 依赖方信任 * 。

   此时将显示依赖方信任列表。
5. 向新创建的依赖方信任添加访问控制策略：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击信任，然后选择 * 编辑访问控制策略 * 。
   c. 选择访问控制策略。
   d. 单击*应用*、然后单击*确定*
6. 将款项申请发放策略添加到新创建的相关方信任：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。
   c. 单击*添加规则*。
   d. 在选择规则模板页面上、从列表中选择*将LDAP属性作为声明发送*、然后单击*下一步*。
   e. 在配置规则页面上，输入此规则的显示名称。

      例如，将 * 对象 GUID 更改为名称 ID* 。
   f. 对于属性存储，选择 * Active Directory* 。
   g. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。
   h. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。
   i. 单击*完成*、然后单击*确定*。
7. 确认元数据已成功导入。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

如果缺少元数据，请确认联合元数据地址是否正确，或者只需手动输入值即可。

8. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。
9. 完成后、返回到StorageGRID 和 "测试所有依赖方信任" 以确认配置正确。

通过导入联合元数据创建依赖方信任

您可以通过访问每个管理节点的 SAML 元数据来导入每个依赖方信任的值。

您需要的内容

- 您已在StorageGRID 中配置SSO、并且知道系统中每个管理节点的完全限定域名(或IP地址)和依赖方标识符。

> 您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

- 您有在 AD FS 中创建依赖方信任的经验，也可以访问 Microsoft AD FS 文档。
- 您正在使用 AD FS 管理单元，并且属于管理员组。

关于此任务

这些说明适用于Windows Server 2016附带的AD FS 4.0。如果您使用的是Windows 2012 R2附带的AD FS 3.0、则会注意到操作步骤 略有不同。如果您有任何疑问，请参见 Microsoft AD FS 文档。

步骤

1. 在Windows Server Manager中、单击*工具*、然后选择* AD FS管理*。
2. 在操作下、单击*添加依赖方信任*。
3. 在Welcome页面上、选择*声明感知*、然后单击*开始*。
4. 选择 * 导入有关依赖方的在线或本地网络上发布的数据 * 。
5. 在 * 联合元数据地址（主机名或 URL ） * 中，键入此管理节点的 SAML 元数据的位置：

   `https://Admin_Node_FQDN/api/saml-metadata`

   适用于 `Admin_Node_FQDN` 下、输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

6. 完成依赖方信任向导，保存依赖方信任并关闭该向导。

> 输入显示名称时，请使用管理节点的相关方标识符，与网格管理器的 Single Sign-On 页面上显示的完全相同。例如： `SG-DC1-ADM1`。

7. 添加声明规则：
   a. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。
   b. 单击*添加规则*：
   c. 在选择规则模板页面上、从列表中选择*将LDAP属性作为声明发送*、然后单击*下一步*。

d. 在配置规则页面上，输入此规则的显示名称。

   例如，将 * 对象 GUID 更改为名称 ID* 。

e. 对于属性存储，选择 * Active Directory* 。

f. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。

g. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。

h. 单击*完成*、然后单击*确定*。

8. 确认元数据已成功导入。

   a. 右键单击依赖方信任以打开其属性。

   b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

      如果缺少元数据，请确认联合元数据地址是否正确，或者只需手动输入值即可。

9. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

10. 完成后、返回到StorageGRID 和 "测试所有依赖方信任" 以确认配置正确。

手动创建依赖方信任

如果您选择不导入依赖部件信任的数据，则可以手动输入值。

您需要的内容

- 您已在StorageGRID 中配置SSO、并且知道系统中每个管理节点的完全限定域名(或IP地址)和依赖方标识符。

  您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

- 您已获得为StorageGRID 管理界面上传的自定义证书、或者知道如何从命令Shell登录到管理节点。
- 您有在 AD FS 中创建依赖方信任的经验，也可以访问 Microsoft AD FS 文档。
- 您正在使用 AD FS 管理单元，并且属于管理员组。

关于此任务

这些说明适用于Windows Server 2016附带的AD FS 4.0。如果您使用的是Windows 2012 R2附带的AD FS 3.0、则会注意到操作步骤 略有不同。如果您有任何疑问，请参见 Microsoft AD FS 文档。

步骤

1. 在Windows Server Manager中、单击*工具*、然后选择* AD FS管理*。
2. 在操作下、单击*添加依赖方信任*。
3. 在Welcome页面上、选择*声明感知*、然后单击*开始*。
4. 选择*手动输入有关依赖方的数据*、然后单击*下一步*。
5. 完成依赖方信任向导：

   a. 输入此管理节点的显示名称。

为了确保一致性，请使用管理节点的依赖方标识符，与网格管理器的单点登录页面上显示的一致。例如：`SG-DC1-ADM1`。

b. 跳过此步骤可配置可选令牌加密证书。

c. 在配置 URL 页面上，选中 * 启用对 SAML 2.0 WebSSO 协议的支持 * 复选框。

d. 键入管理节点的 SAML 服务端点 URL：

`https://Admin_Node_FQDN/api/saml-response`

适用于 `Admin_Node_FQDN` 下、输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

e. 在配置标识符页面上，指定同一管理节点的依赖方标识符：

`Admin_Node_Identifier`

适用于 `Admin_Node_Identifier` 下、输入管理节点的依赖方标识符、与单点登录页面上显示的完全相同。例如：`SG-DC1-ADM1`。

f. 查看设置，保存依赖方信任并关闭向导。

此时将显示编辑款项申请发放策略对话框。

如果未显示此对话框，请右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。

6. 要启动声明规则向导、请单击*添加规则*：

a. 在选择规则模板页面上、从列表中选择*将LDAP属性作为声明发送*、然后单击*下一步*。

b. 在配置规则页面上，输入此规则的显示名称。

例如，将 * 对象 GUID 更改为名称 ID* 。

c. 对于属性存储，选择 * Active Directory* 。

d. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。

e. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。

f. 单击*完成*、然后单击*确定*。

7. 右键单击依赖方信任以打开其属性。

8. 在 * 端点 * 选项卡上，为单点注销（ SLO ）配置端点：

a. 单击*添加SAML *。

b. 选择 * 端点类型 * > * SAML 注销 * 。

c. 选择 * 绑定 * > * 重定向 * 。

d. 在 * 可信 URL* 字段中，输入用于从此管理节点单点注销（ SLO ）的 URL：

`https://Admin_Node_FQDN/api/saml-logout`

适用于 `*Admin_Node_FQDN*`下、输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

a. 单击 * 确定 * 。

9. 在 * 签名 * 选项卡上，指定此依赖方信任的签名证书：

a. 添加自定义证书：

- 如果您已将自定义管理证书上传到 StorageGRID ，请选择此证书。
- 如果您没有自定义证书、请登录到管理节点、然后转到 `/var/local/mgmt-api` 管理节点的目录、然后添加 `custom-server.crt` 证书文件。

*注：*使用管理节点的默认证书 (`server.crt`)。如果管理节点出现故障，则在恢复节点时将重新生成默认证书，您需要更新依赖方信任。

b. 单击*应用*、然后单击*确定*。

依赖方属性将被保存并关闭。

10. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。
11. 完成后、返回到StorageGRID 和 "测试所有依赖方信任" 以确认配置正确。

测试依赖方信任

在对StorageGRID 强制使用单点登录(SSO)之前、请确认已正确配置单点登录和单点注销(SLO)。如果您为每个管理节点创建了依赖方信任、请确认您可以对每个管理节点使用SSO和SLO。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 您已在AD FS中配置一个或多个依赖方信任。

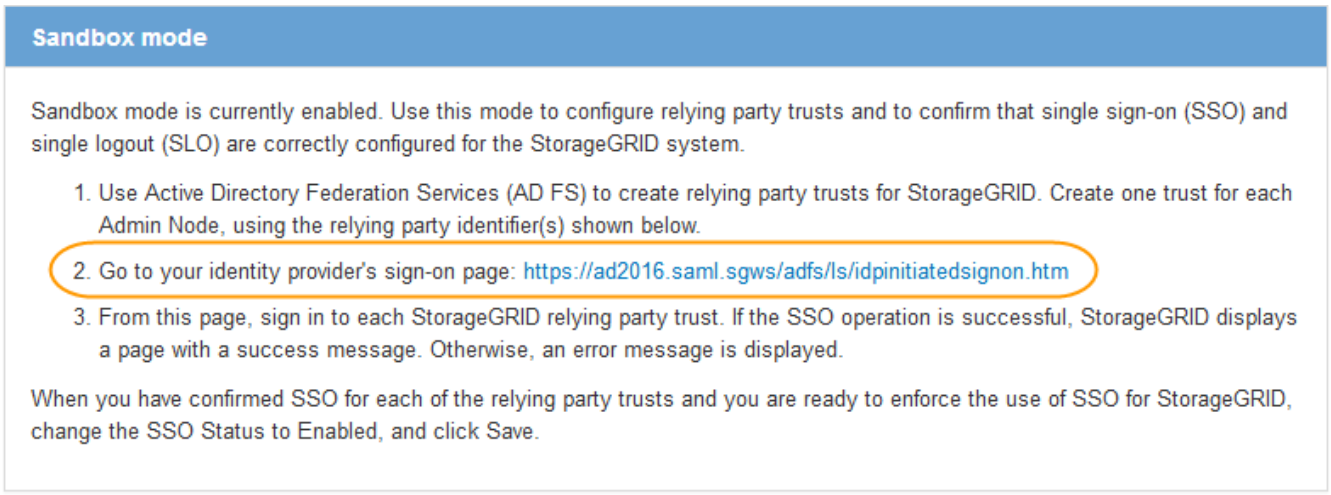
步骤

1. 选择*配置访问控制单点登录*。

此时将显示Single Sign-On页面、并选择了*沙盒模式*选项。

2. 在沙盒模式说明中、找到指向身份提供程序登录页面的链接。

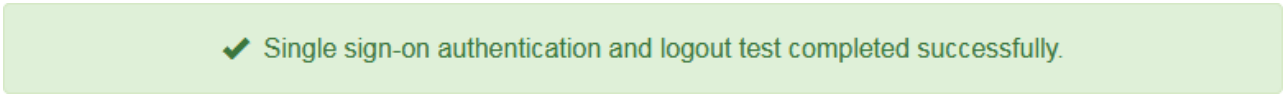
此URL是从您在*联合服务名称*字段中输入的值派生的。



3. 单击此链接、或者将此URL复制并粘贴到浏览器中、以访问身份提供程序的登录页面。
4. 要确认您可以使用SSO登录到StorageGRID 、请选择*登录到以下站点之一*、选择主管理节点的依赖方标识符、然后单击*登录*。

系统将提示您输入用户名和密码。

5. 输入您的联合用户名和密码。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。



   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
6. 重复上述步骤以确认您可以登录到任何其他管理节点。

如果所有SSO登录和注销操作均成功、则可以启用SSO。

启用单点登录

在使用沙盒模式测试所有StorageGRID 依赖方信任之后、您可以启用单点登录(SSO)。

您需要的内容

- 您必须已从身份源导入至少一个联合组、并已将root访问管理权限分配给该组。对于任何现有租户帐户、您必须确认至少有一个联合用户对网格管理器和租户管理器具有root访问权限。
- 您必须已使用沙盒模式测试所有依赖方信任。

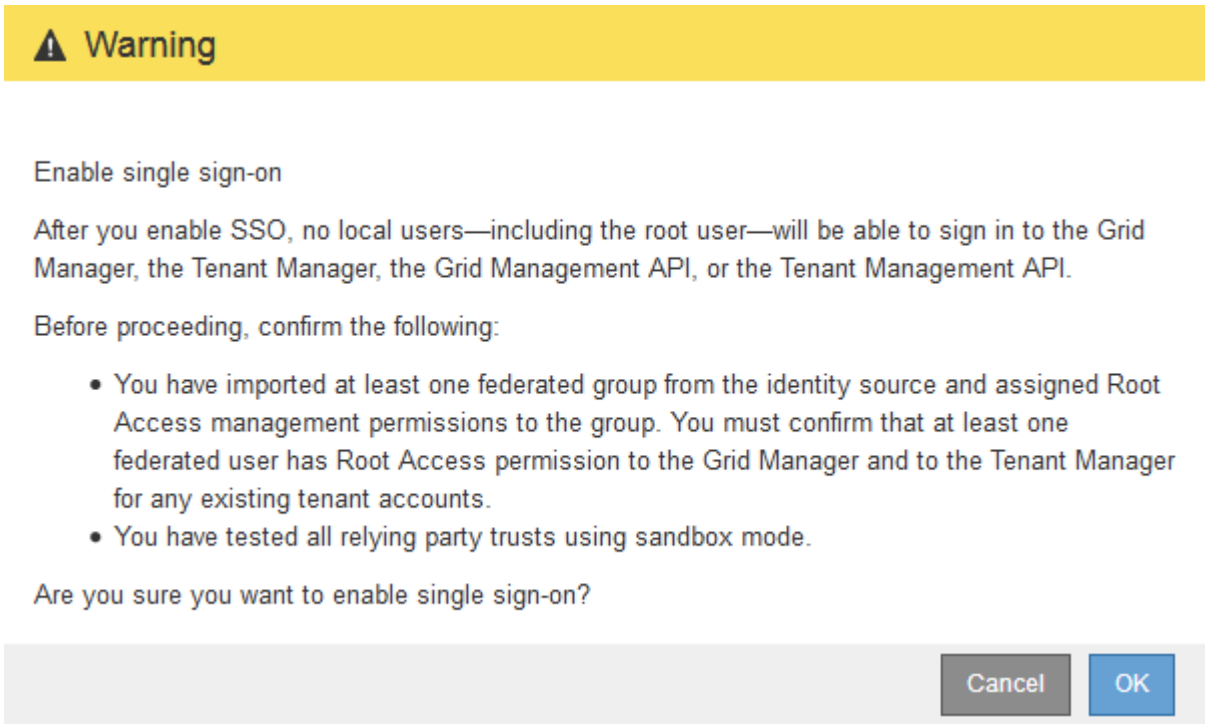
步骤

1. 选择*配置访问控制单点登录*。

   此时将显示Single Sign-On页面、并选择了*沙盒模式*。

2. 将 SSO 状态更改为 * 已启用 * 。
3. 单击 * 保存 * 。

   此时将显示一条警告消息。



4. 查看警告、然后单击*确定*。

   现在，已启用单点登录。

> 所有用户都必须使用SSO访问网格管理器、租户管理器、网格管理API和租户管理API。本地用户无法再访问 StorageGRID 。

禁用单点登录

如果您不再希望使用单点登录（ SSO ）功能，则可以禁用此功能。必须先禁用单点登录，然后才能禁用身份联合。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。

- 您必须具有特定的访问权限。

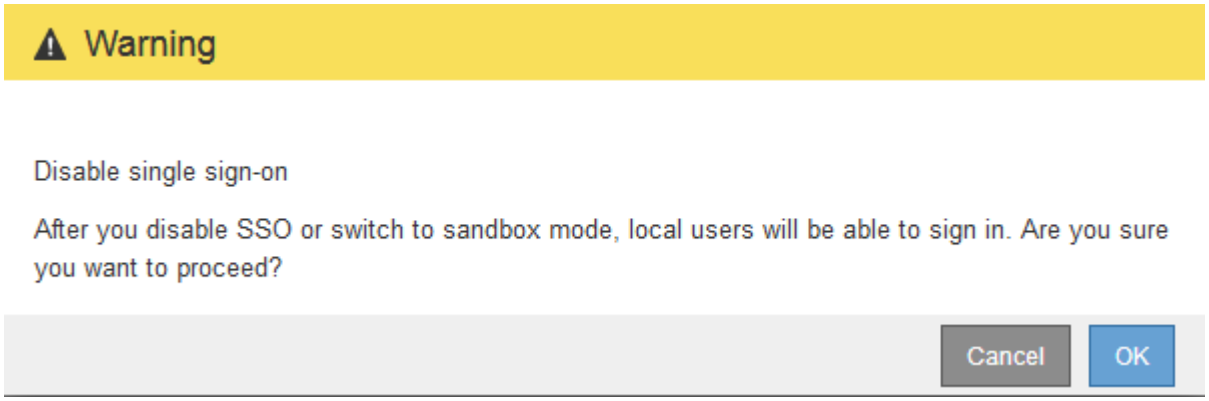
步骤

1. 选择*配置访问控制单点登录*。

   此时将显示 Single Sign-On 页面。

2. 选择 * 已禁用 * 选项。
3. 单击 * 保存 * 。

   此时将显示一条警告消息，指示本地用户现在可以登录。



4. 单击 * 确定 * 。

   下次登录到 StorageGRID 时，将显示 StorageGRID 登录页面，您必须输入本地或联合 StorageGRID 用户的用户名和密码。

临时禁用并重新启用一个管理节点的单点登录

如果单点登录（ Single Sign-On ， SSO ）系统发生故障，您可能无法登录到网格管理器。在这种情况下，您可以为一个管理节点临时禁用并重新启用 SSO 。要禁用并重新启用 SSO ，必须访问节点的命令 Shell 。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `Passwords.txt` 文件
- 您必须知道本地root用户的密码。

关于此任务

为一个管理节点禁用 SSO 后，您可以以本地 root 用户身份登录到网格管理器。要保护 StorageGRID 系统的安全，您必须在注销后立即使用节点的命令 Shell 在管理节点上重新启用 SSO 。

> 为一个管理节点禁用 SSO 不会影响网格中任何其他管理节点的 SSO 设置。网格管理器的单点登录页面上的 * 启用 SSO* 复选框将保持选中状态，并且所有现有的 SSO 设置都将保持不变，除非您对其进行更新。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

      以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 运行以下命令：`disable-saml`

   此时将显示一条消息，指出命令适用场景 this Admin Node only 。

3. 确认要禁用 SSO 。

   显示一条消息，指示节点上已禁用单点登录。

4. 从 Web 浏览器访问同一管理节点上的网格管理器。

   现在，由于已禁用 SSO ，将显示网格管理器登录页面。

5. 使用用户名 root 和本地 root 用户的密码登录。
6. 如果您因需要更正 SSO 配置而临时禁用 SSO ：
   a. 选择*配置访问控制单点登录*。
   b. 更改不正确或过时的 SSO 设置。
   c. 单击 * 保存 * 。

      单击Single Sign-On页面中的*保存*会自动为整个网格重新启用SSO。

7. 如果您因某些其他原因需要访问网格管理器而临时禁用 SSO ：
   a. 执行需要执行的任何任务。
   b. 单击*注销*、然后关闭网格管理器。
   c. 在管理节点上重新启用 SSO 。您可以执行以下任一步骤：

      - 运行以下命令： `enable-saml`

        此时将显示一条消息，指出命令适用场景 this Admin Node only 。

      确认要启用 SSO 。

   显示一条消息，指示节点上已启用单点登录。

   - 重新启动网格节点： `reboot`

8. 从 Web 浏览器中，从同一管理节点访问网格管理器。

9. 确认此时将显示 StorageGRID 登录页面，并且您必须输入 SSO 凭据才能访问网格管理器。

相关信息

"配置单点登录"

配置管理员客户端证书

您可以使用客户端证书允许授权的外部客户端访问StorageGRID Prometheus数据库。客户端证书提供了一种使用外部工具监控StorageGRID 的安全方式。

如果您需要使用外部监控工具访问StorageGRID 、则必须使用网格管理器上传或生成客户端证书、并将证书信息复制到外部工具。

添加管理员客户端证书

要添加客户端证书、您可以提供自己的证书或使用网格管理器生成一个证书。

您需要的内容

- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须知道管理节点的IP地址或域名。
- 您必须已配置StorageGRID 管理接口服务器证书并具有相应的CA包
- 如果要上传您自己的证书、则本地计算机上必须提供此证书的公有 密钥和专用密钥。

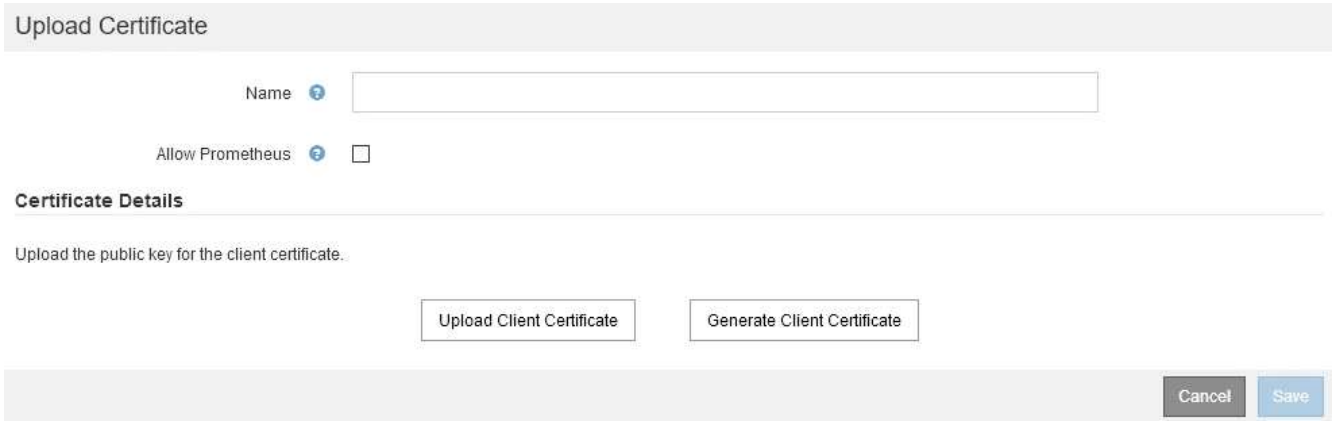
步骤

1. 在网格管理器中、选择*配置*>*访问控制*>*客户端证书*。

   此时将显示客户端证书页面。

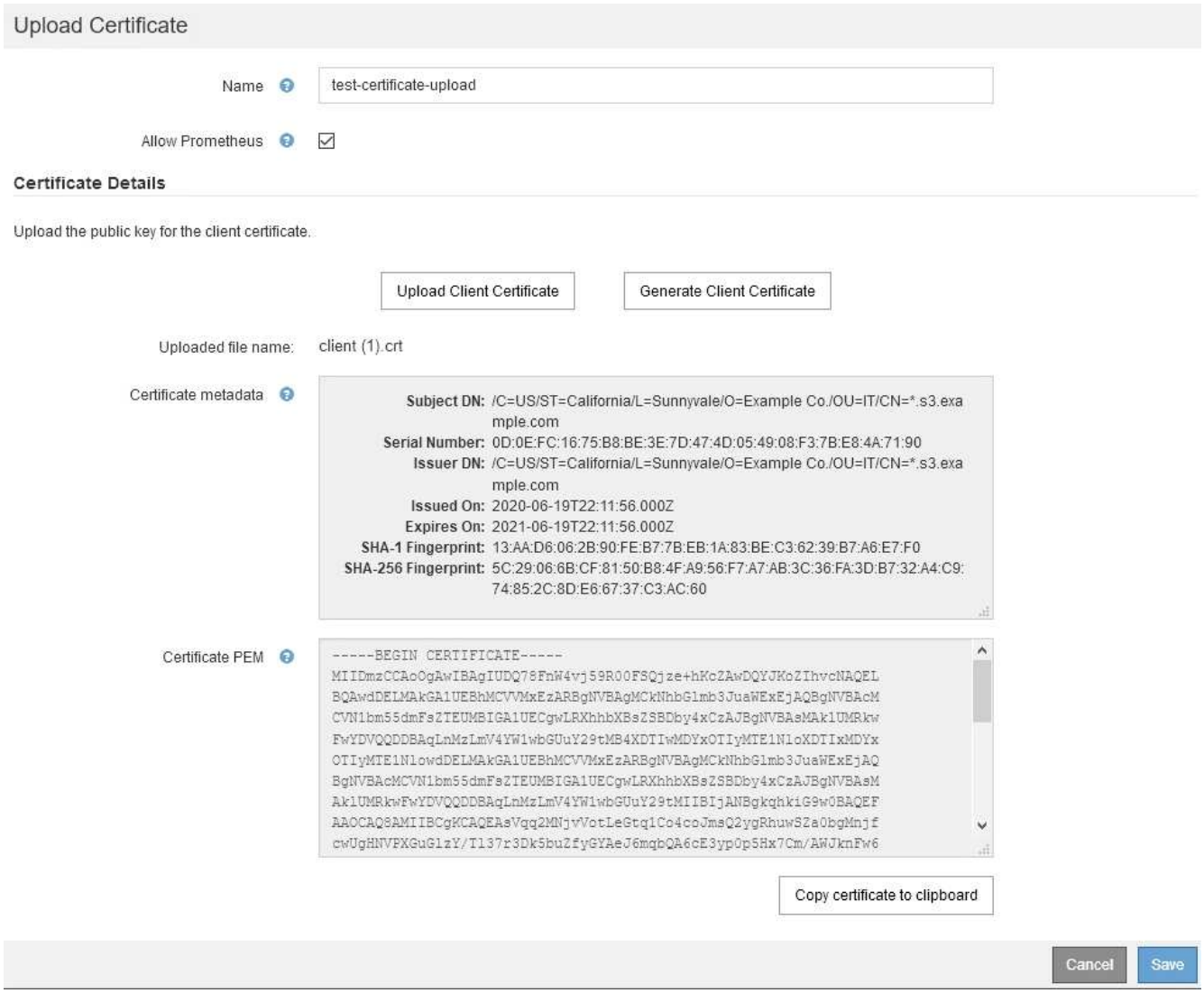
2. 选择 * 添加 * 。

   此时将显示上传证书页面。



3. 键入一个介于1到32个字符之间的证书名称。
4. 要使用外部监控工具访问Prometheus指标、请选中*允许Prometheus*复选框。
5. 上传或生成证书：
   a. 要上传证书、请转至 此处。
   b. 要生成证书、请转至 此处。
6. 要上传证书、请执行以下操作：
   a. 选择*上传客户端证书*。
   b. 浏览此证书的公有 密钥。

      上传证书的公有 密钥后、系统将填充*证书元数据*和*证书PEM*字段。



a. 选择*将证书复制到剪贴板*、然后将证书粘贴到外部监控工具中。

b. 使用编辑工具将私钥复制并粘贴到外部监控工具中。

c. 选择*保存*以在网格管理器中保存证书。

7. 要生成证书、请执行以下操作：

a. 选择*生成客户端证书*。

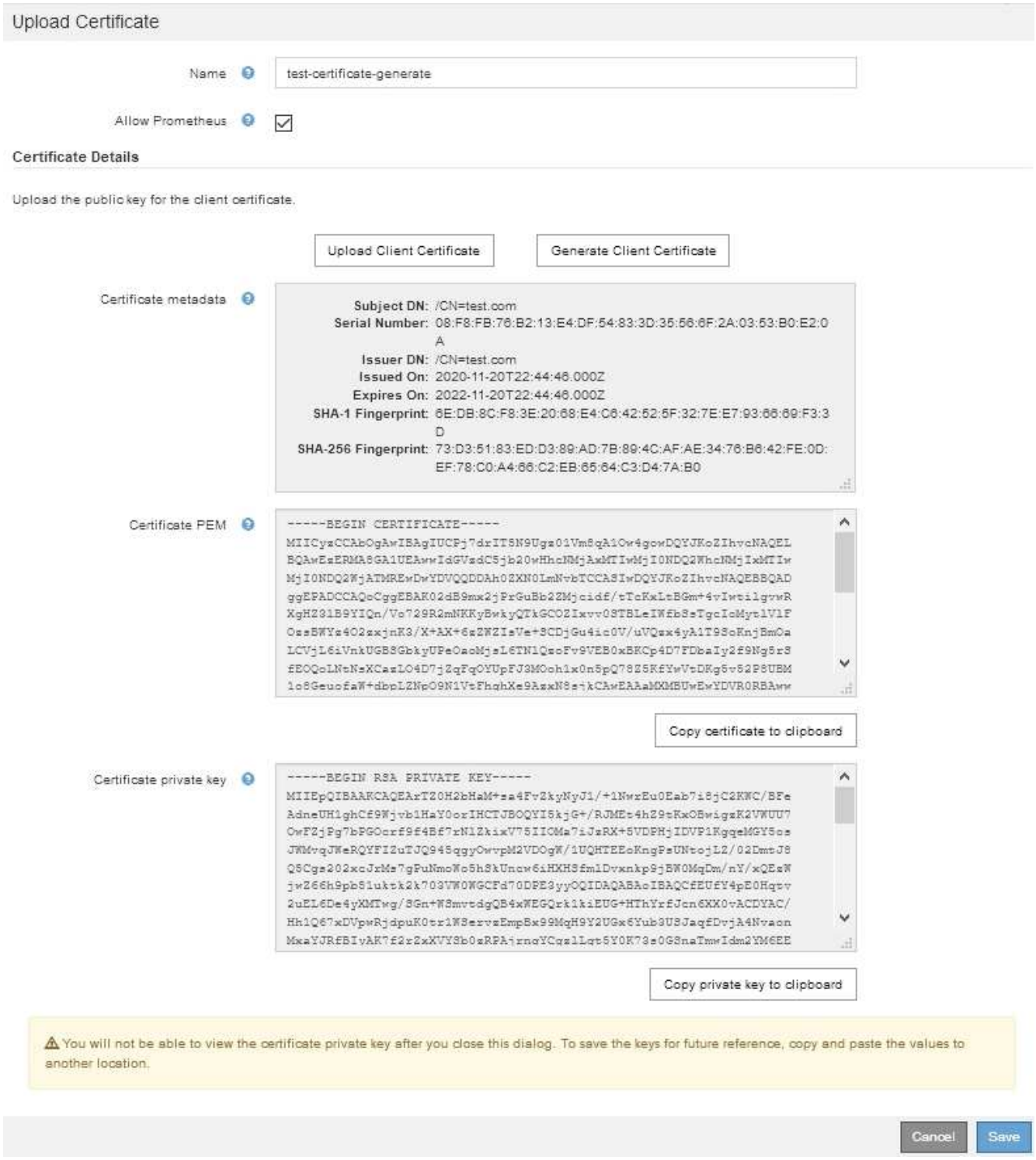
b. 输入管理节点的域名或IP地址。

c. (可选)输入一个X.509主题(也称为可分辨名称(Distinguished Name、DN))、以确定拥有证书的管理员。

d. (可选)选择证书的有效天数。默认值为730天。

e. 选择 * 生成 * 。

此时将填充*证书元数据*、*证书PEM*和*证书专用密钥*字段。



a. 选择*将证书复制到剪贴板*、然后将证书粘贴到外部监控工具中。

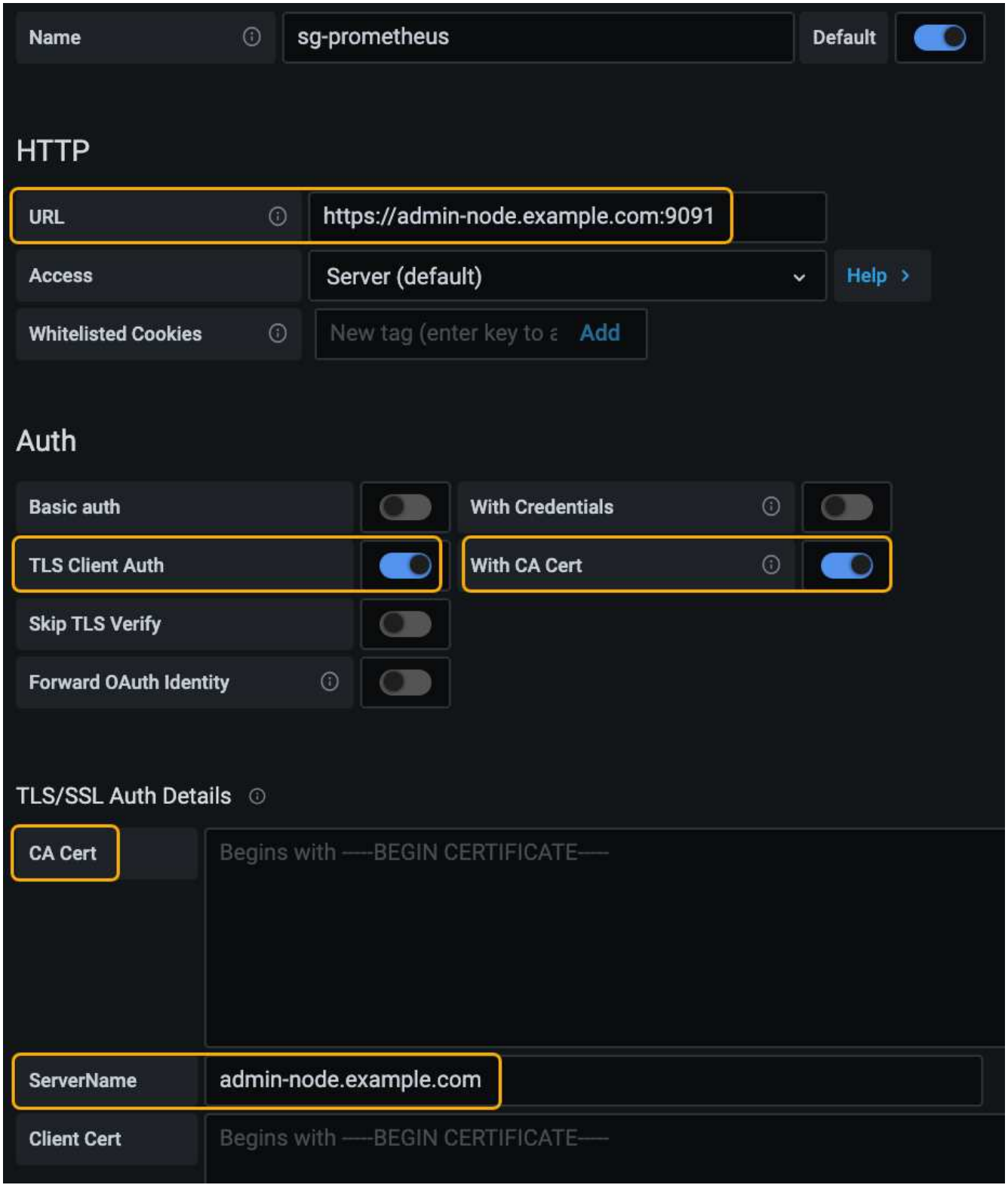
b. 选择*将私钥复制到剪贴板*、然后将密钥粘贴到外部监控工具中。

> 关闭此对话框后、您将无法查看此私钥。将密钥复制到安全位置。

c. 选择*保存*以在网格管理器中保存证书。

8. 在外部监控工具上配置以下设置，例如 Grafana 。

以下屏幕截图显示了一个 Grafana 示例：



a. * 名称 * ： 输入连接的名称。

   StorageGRID 不需要此信息，但您必须提供一个名称来测试连接。

b. * URL * ： 输入管理节点的域名或 IP 地址。指定 HTTPS 和端口 9091 。

例如： `https://admin-node.example.com:9091`

c. 启用* TLS客户端授权*和*使用CA证书*。

d. 将管理接口服务器证书或CA捆绑包复制并粘贴到TLS/SSL身份验证详细信息下的"CA证书"中。

e. * 服务器名称 * ： 输入管理节点的域名。

服务器名称必须与管理接口服务器证书中显示的域名匹配。

f. 保存并测试从 StorageGRID 或本地文件复制的证书和私钥。

现在，您可以使用外部监控工具从 StorageGRID 访问 Prometheus 指标。

有关指标的信息、请参见StorageGRID 监控和故障排除说明。

相关信息

"使用StorageGRID 安全证书"

"为网格管理器和租户管理器配置自定义服务器证书"

"监控和放大；故障排除"

编辑管理员客户端证书

您可以编辑证书以更改其名称、启用或禁用Prometheus访问、或者在当前证书已过期时上传新证书。

您需要的内容

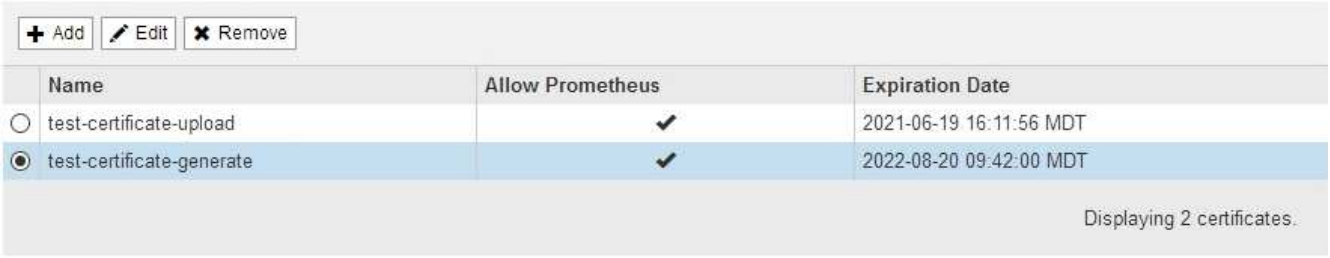
- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须知道管理节点的IP地址或域名。
- 如果您要上传新证书和私钥、它们必须在本地计算机上可用。

步骤

1. 选择*配置*>*访问控制*>*客户端证书*。

此时将显示客户端证书页面。此时将列出现有证书。

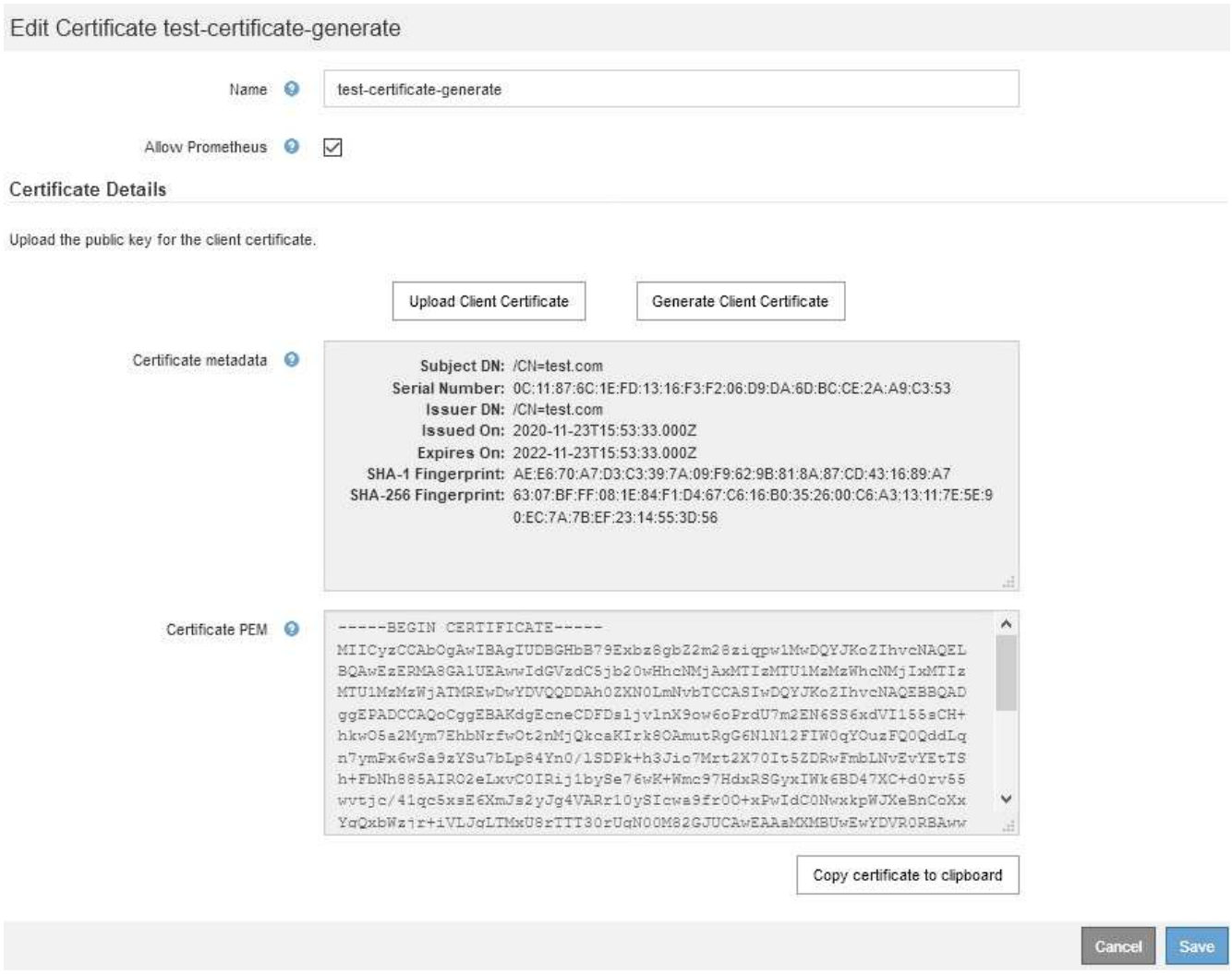
表中列出了证书到期日期。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。



2. 选择要编辑的证书左侧的单选按钮。

3. 选择 * 编辑 * 。

此时将显示编辑证书对话框。



4. 对证书进行所需的更改。
5. 选择*保存*以在网格管理器中保存证书。
6. 如果您上传了新证书：
   a. 选择*将证书复制到剪贴板*将证书粘贴到外部监控工具。
   b. 使用编辑工具将新的私钥复制并粘贴到外部监控工具中。
   c. 在外部监控工具中保存并测试证书和私钥。
7. 如果生成了新证书：
   a. 选择*将证书复制到剪贴板*将证书粘贴到外部监控工具。
   b. 选择*将私钥复制到剪贴板*将证书粘贴到外部监控工具。

      关闭此对话框后、您将无法查看或复制此私钥。将密钥复制到安全位置。

   c. 在外部监控工具中保存并测试证书和私钥。

正在删除管理员客户端证书

如果您不再需要证书、可以将其删除。

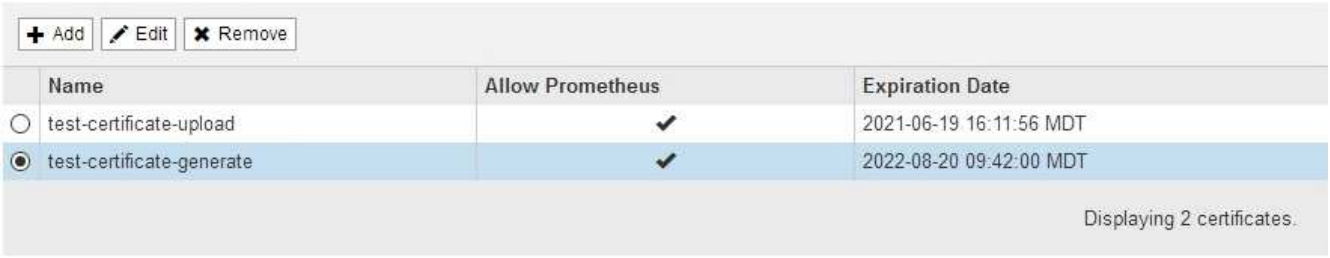
您需要的内容

- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

步骤

1. 选择*配置*>*访问控制*>*客户端证书*。

   此时将显示客户端证书页面。此时将列出现有证书。



2. 选择要删除的证书左侧的单选按钮。
3. 选择 * 删除 * 。

   此时将显示确认对话框。

4. 选择 * 确定 * 。

   此证书将被删除。