控制对 StorageGRID 的访问

StorageGRID software

NetApp
July 23, 2026

目录

控制对 StorageGRID 的访问

控制 StorageGRID 访问

您可以通过创建或导入组和用户并为每个组分配权限来控制谁可以访问 StorageGRID 以及用户可以执行哪些任务。也可以启用单点登录 (SSO)、创建客户端证书和更改网格密码。

控制对 Grid Manager 的访问

您可以通过从身份联合服务导入组和用户，或通过设置本地组和本地用户来确定谁可以访问 Grid Manager 和网格管理 API。

使用"身份联合"可以加快设置"groups"和"用户"的速度，并允许用户使用熟悉的凭据登录 StorageGRID。如果使用 Active Directory、OpenLDAP 或 Oracle Directory Server，则可以配置身份联合。

> 如果要使用其他 LDAP v3 服务，请联系技术支持。

您可以通过为每个组分配不同的"权限"权限来确定每个用户可以执行哪些任务。例如，您可能希望一个组中的用户能够管理 ILM 规则，而另一个组中的用户能够执行维护任务。用户必须至少属于一个组才能访问系统。

或者，您可以将组配置为只读。只读组中的用户只能查看设置和功能。他们无法在 Grid Manager 或 Grid Management API 中进行任何更改或执行任何操作。

启用单点登录

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)。在您"配置并启用 SSO"之后，所有用户都必须通过外部身份提供程序的身份验证，然后才能访问 Grid Manager、Tenant Manager、网格管理 API 或租户管理 API。本地用户无法登录 StorageGRID。

更改配置密码短语

许多安装和维护过程以及下载 StorageGRID 恢复包都需要配置密码。下载 StorageGRID 系统的网格拓扑信息和加密密钥的备份也需要密码。您可以根据需要"更改密码短语"。

更改节点控制台密码

网格中的每个节点都有一个节点控制台密码，您需要使用 SSH 以"admin"身份登录到节点，或通过 VM/物理控制台连接登录到 root 用户。根据需要，您可以"更改节点控制台密码"针对每个节点。

更改 StorageGRID 配置密码

使用此过程更改 StorageGRID 配置密码。恢复、扩展和维护过程均需要此密码短语。下载恢复包备份时也需要此密码短语，恢复包备份中包含 StorageGRID 系统的网格拓扑信息、网格节点控制台密码和加密密钥。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

- ${post_edited_translations.segment}
- 您有当前的设置密码短语。

关于此任务

许多安装和维护程序以及 "${post_edited_translations.segment}" 都需要配置密码。配置密码未在 `Passwords.txt` 文件中列出。请务必记录配置密码并将其保存在安全的位置。

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. 输入新的密码短语。密码短语必须包含至少 8 个且不超过 32 个字符。密码短语区分大小写。

   将配置密码短语存储在安全位置。这是安装、扩展和维护程序所必需的。

5. 重新输入新密码，然后选择*Save*。

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. 输入新的配置密码短语以下载新的恢复包。

   更改配置密码后，必须立即下载新的恢复包。恢复包文件允许您在发生故障时还原系统。

在 StorageGRID 中更改节点控制台密码

网格中的每个节点都有一个节点控制台密码，用于登录到该节点。默认情况下，每个节点都有一个唯一的密码。您可以将每个密码更改为新的唯一密码，也可以将每个节点的密码更改为使用全局密码。密码存储在恢复包中。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。
- 您有当前的设置密码短语。

关于此任务

您可以使用节点控制台密码通过 SSH 以"admin"身份登录到节点，或通过 VM/物理控制台连接登录到 root 用户。您可以使用以下选项之一更改节点控制台密码：

- 自动将随机密码应用到每个节点
- 指定一个全局密码并将其应用于所有节点

- 指定唯一密码并将其应用于一个或多个节点

密码存储在恢复包的更新 `Passwords.txt`文件中。密码列在文件的"Password"列中。

> 用于节点之间通信的 SSH 密钥的 "SSH 访问密码" 与节点控制台密码分开。此过程不会更改 SSH 访问密码。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 网格密码。
2. 在*更改节点控制台密码*下，选择*进行更改*。

下载当前恢复包

在更改节点控制台密码之前，请下载当前恢复包。如果任何节点的密码更改过程失败，您可以使用此文件中的密码。

步骤

1. 输入网格的配置密码短语。
2. 选择*下载恢复软件包*。
3. 将恢复包文件 (`.zip`) 复制到两个安全、可靠且分开的位置。

> 必须保护恢复包文件，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

4. 选择 **Continue**。

提供新密码

1. 请选择要使用的密码更改方法。
   - 自动：StorageGRID 会自动为所有节点分配新的随机控制台密码。
   - **Custom**：您提供控制台密码。

自动

1. 选择 **Continue**。

自定义

1. 选择以下选项之一：
   - 全局控制台密码：对所有节点应用相同的控制台密码。
   - 唯一控制台密码：在一个或多个节点上应用不同的密码。
2. 如果选择*全局控制台密码*，请输入要用于所有节点的密码。
3. 如果您选择了*Unique console passwords*，请输入一个或多个节点的唯一密码。
4. 选择 **Continue**。

完成密码更改

1. 出现确认对话框时，如果您已准备好让 StorageGRID 开始更改节点控制台密码，请选择 **Yes**。

   此流程开始后，您无法取消。

   StorageGRID 生成包含新密码的新恢复包。

2. 当新的恢复包准备就绪时，选择 **Download new recovery package** 并保存恢复包。
3. 打开 `.zip`文件。
4. 确认您可以访问内容，包括 `Passwords.txt`文件，该文件包含新节点控制台密码。
5. 将新的恢复包文件 (`.zip` 复制到两个安全、可靠且独立的位置。

   不要覆盖旧的恢复软件包。

   您必须保护恢复文件，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

6. 选中复选框以指示您已下载新的恢复包并验证了内容。
7. 选择 **Continue**。

   StorageGRID 更新每个节点的密码。

   如果在更新过程中出现错误，进度条会列出未能更改密码的节点数量。系统将自动在无法更改密码的任何节点上重试该过程。如果过程结束时某些节点仍未更改密码，则会出现 **Retry** 按钮。

8. 如果一个或多个节点的密码更新失败：
   a. 查看表中列出的错误消息。
   b. 解决问题。
   c. 选择*重试*。

重试仅更改之前密码更改尝试失败的节点上的节点控制台密码。

9. 当进度条指示没有剩余更新时，选择 **Finish**。
10. 更改所有节点的节点控制台密码后，删除您下载的第一个恢复包。

更改 StorageGRID 管理节点的 SSH 访问密码

更改管理节点的 SSH 访问密码还会更新网格中每个节点的唯一内部 SSH 密钥集。主管理节点使用这些 SSH 密钥通过安全的无密码身份验证访问节点。

使用 SSH 密钥以 `admin`身份登录节点，或以 root 用户身份登录虚拟机或物理控制台连接。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。
- 您有当前的设置密码短语。

关于此任务

管理节点的新访问密码和每个节点的新内部密钥存储在恢复包中的 `Passwords.txt`文件中。密钥列在该文件的"密码"列中。

用于节点之间通信的 SSH 密钥有单独的 SSH 访问密码。这些密码不会通过此程序进行更改。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 网格密码。
2. 在 **Change SSH keys** 下，选择 **Make a change**。

下载当前恢复包

在更改 SSH 访问密钥之前，请下载当前恢复包。如果任何节点的密钥更改过程失败，您可以使用此文件中的密钥。

步骤

1. 输入网格的配置密码短语。
2. 选择*下载恢复软件包*。
3. 将恢复包文件 (`.zip`) 复制到两个安全、可靠且分开的位置。

必须保护恢复包文件，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

4. 选择 **Continue**。
5. 出现确认对话框时，如果您已准备好开始更改 SSH 访问密钥，请选择 是。

此流程开始后，您无法取消。

更改 SSH 访问密钥

当更改 SSH 访问密钥过程开始时，将生成包含新密钥的新恢复包。然后，在每个节点上更新密钥。

步骤

1. 等待生成新的恢复包，这可能需要几分钟时间。
2. 启用下载新恢复包按钮后，选择*下载新恢复包*并将新恢复包文件(`.zip`保存到两个安全、可靠且分开的位置。
3. 下载完成后：

   a. 打开 `.zip`文件。

   b. 确认您可以访问内容，包括包含新 SSH 访问密钥的 `Passwords.txt`文件。

   c. 将新的恢复包文件 (`.zip` 复制到两个安全、可靠且独立的位置。

   不要覆盖旧的恢复软件包。

   必须保护恢复包文件，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

4. 等待每个节点上的密钥更新，这可能需要几分钟时间。

   如果更改了所有节点的密钥，则会显示绿色成功横幅。

   如果在更新过程中出现错误，横幅消息将列出未能更改其密钥的节点数量。系统将自动在任何未能更改其密钥的节点上重试该过程。如果过程结束时某些节点仍然没有更改密钥，则会出现 **Retry** 按钮。

   如果一个或多个节点的密钥更新失败：

   a. 查看表中列出的错误消息。

   b. 解决问题。

   c. 选择*重试*。

      重试仅更改在先前密钥更改尝试期间失败的节点上的 SSH 访问密钥。

5. 更改所有节点的 SSH 访问密钥后，请删除 您下载的第一个恢复包。
6. （可选）选择 **Maintenance** > **System** > **Recovery package** 以下载新恢复包的其他副本。

在 StorageGRID 中使用身份联合

使用身份联合可以更快地设置组和用户，并允许用户使用熟悉的凭据登录 StorageGRID。

为 Grid Manager 配置身份联合

如果您希望在 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 等其他系统中管理

管理组和用户，则可以在 Grid Manager 中配置身份联合。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您已完成 "特定访问权限"。
- 您正在使用 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

  如果希望使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP，则必须配置 OpenLDAP 服务器。请参阅 配置 OpenLDAP 服务器的指南。
- 如果您计划启用单一登录 (SSO)，则已阅读 "单点登录的要求和注意事项"。
- 如果您计划使用传输层安全 (TLS) 与 LDAP 服务器进行通信，则身份提供程序正在使用 TLS 1.2 或 1.3。请参阅 "传出 TLS 连接支持的密码"。

关于此任务

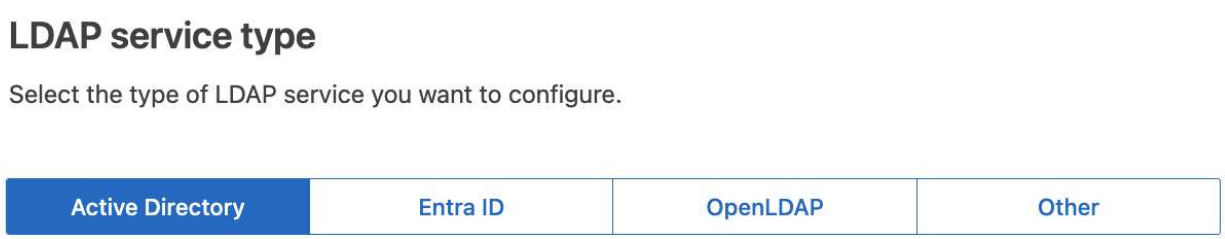
如果要从其他系统（如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）导入组，则可以为网格管理器配置身份源。您可以导入以下类型的组：

- 管理员组。管理员组中的用户可以根据分配给该组的管理权限登录到 Grid Manager 并执行任务。
- 不使用自己的身份源的租户的租户用户组。租户组中的用户可以根据在租户管理器中分配给该组的权限登录到租户管理器并执行任务。请参阅"创建租户帐户"和"使用租户帐户"了解详情。

输入配置

步骤

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



选择*其他*以配置使用 Oracle Directory Server 的 LDAP 服务器的值。

4. 如果您选择了*其他*，请填写 LDAP 属性部分中的字段。否则，请转至下一步。
   - 用户唯一名称：包含 LDAP 用户唯一标识符的属性名称。此属性等效于 Active Directory 的 `sAMAccountName`和 `OpenLDAP` 的 `uid`。如果要配置 Oracle Directory Server，请输入 `uid`。
   - 用户 **UUID**：包含 LDAP 用户永久唯一标识符的属性名称。此属性等效于 Active Directory 的

`objectGUID`和 `OpenLDAP` 的 `entryUUID`。如果要配置 Oracle Directory Server，请输入 `nsuniqueid`。每个用户的指定属性值必须是 16 字节或字符串格式的 32 位十六进制数字，其中连字符将被忽略。

- 组唯一名称：包含 LDAP 组唯一标识符的属性名称。此属性等效于 Active Directory 的 `sAMAccountName`和 `OpenLDAP` 的 `cn`。如果要配置 Oracle Directory Server，请输入 `cn`。
- 组 **UUID**：包含 LDAP 组的永久唯一标识符的属性名称。此属性等效于 Active Directory 的 `objectGUID`和 `OpenLDAP` 的 `entryUUID`。如果要配置 Oracle Directory Server，请输入 `nsuniqueid`。每个组的指定属性值必须是 16 字节或字符串格式的 32 位十六进制数字，其中连字符将被忽略。

5. 对于所有 LDAP 服务类型，请在"配置 LDAP 服务器"部分中输入所需的 LDAP 服务器和网络连接信息。
   - 主机名：LDAP 服务器的完全限定域名 (FQDN) 或 IP 地址。
   - 端口：用于连接到 LDAP 服务器的端口。

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

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

     对于 Active Directory，还可以指定下层登录名称或用户主体名称。

     指定的用户必须具有列出组和用户以及访问以下属性的权限：

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

   - 密码：与用户名关联的密码。

     如果以后更改密码，则必须在此页面上进行更新。

   - **Group Base 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，其可分辨名称相对于基本 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。

   - 用户群 **DN**：要搜索用户的 LDAP 子树的标识名 (DN) 的完整路径。

     用户唯一名称*值在其所属的*用户基础 **DN** 中必须是唯一的。

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

建议提供*绑定用户名格式*，因为如果 StorageGRID 无法与服务帐户绑定，它仍可允许用户登录。

输入以下模式之一：

- **UserPrincipalName** 模式（**AD** 和 **Entra ID**）： `[USERNAME]@example.com`
- 下级登录名称模式（**AD** 和 **Entra ID**）： `example\[USERNAME]`
- 辨识名模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

请按原样填写 **[USERNAME]**。

6. 在传输层安全性 (TLS) 部分，选择一个安全设置。
   - 使用 **STARTTLS**：使用 STARTTLS 保护与 LDAP 服务器的通信。这是 Active Directory、OpenLDAP 或其他选项的推荐选项，但 Microsoft Entra ID 不支持此选项。
   - 使用 **LDAPS**：LDAPS（LDAP over SSL）选项使用 TLS 建立与 LDAP 服务器的连接。您必须为 Microsoft Entra ID 选择此选项。
   - 不使用 **TLS**：StorageGRID 系统与 LDAP 服务器之间的网络流量将不受保护。Microsoft Entra ID 不支持此选项。

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

7. 如果选择了 STARTTLS 或 LDAPS，请选择用于保护连接的证书。
   - **Use operating system CA certificate**：使用操作系统上安装的默认网格 CA 证书来保护连接。
   - 使用自定义 **CA** 证书：使用自定义安全证书。

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

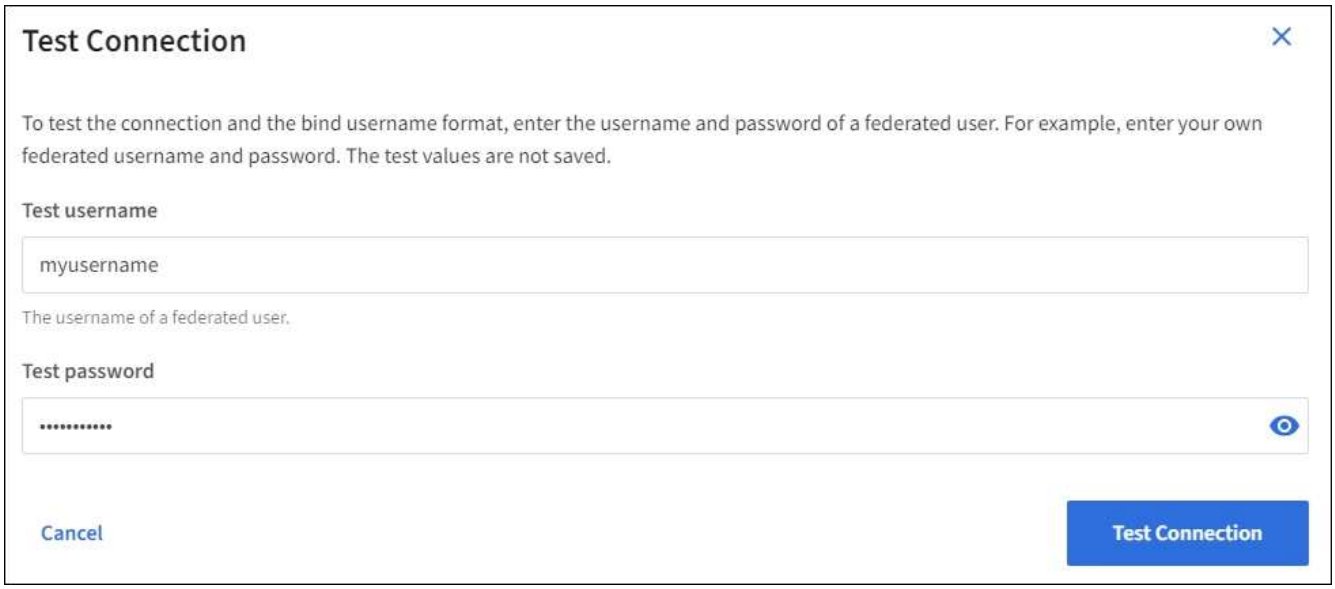
测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。StorageGRID 验证 LDAP 服务器的连接设置以及绑定用户名格式（如果已提供）。

步骤

1. 选择*测试连接*。
2. 如果未提供绑定用户名格式：
   - 如果连接设置有效，则会显示"Test connection successful"（测试连接成功）消息。选择 **Save** 保存配置。
   - 如果连接设置无效，将显示"无法建立测试连接"消息。选择*Close*。然后，解决任何问题并再次测试连接。
3. 如果您提供了绑定用户名格式，请输入有效的联合用户的用户名和密码。

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



- 如果连接设置有效，则会显示"Test connection successful"（测试连接成功）消息。选择 **Save** 保存配置。
- 如果连接设置、绑定用户名格式或测试用户名和密码无效，则会显示错误消息。请解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统定期从身份源同步联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到"身份联合"页面。
2. 选择页面顶端的*同步服务器*。

   同步过程可能需要一段时间，具体取决于您的环境。

   如果从身份源同步联合组和用户时出现问题，则会触发*身份联合同步失败*警报。

禁用身份联合

您可以暂时或永久禁用组和用户的身份联合。禁用身份联合后，StorageGRID 与身份源之间将不再进行通信。但是，您已配置的所有设置将被保留，以便将来可以轻松重新启用身份联合。

关于此任务

在禁用身份联合之前，应注意以下事项：

- 联合用户将无法登录。
- 当前登录的联合用户将在其会话过期之前保留对 StorageGRID 系统的访问权限，但在其会话过期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，也不会针对尚未同步的帐户发出警报。
- 如果单点登录 (SSO) 状态为*已启用*或*沙盒模式*，则*启用身份联合*复选框将被禁用。必须先将单点登录页面上的 SSO 状态设置为*已禁用*，然后才能禁用身份联合。请参阅 "禁用单点登录"。

步骤

1. 转到"身份联合"页面。
2. 取消选中*启用身份联合*复选框。

配置 OpenLDAP 服务器的指南

如果要将 OpenLDAP 服务器用于身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于不是 Active Directory 或 Microsoft Entra ID 的身份源，StorageGRID 不会自动阻止对外部禁用的用户进行 S3 访问。要阻止 S3 访问，请删除该用户的任何 S3 密钥或从所有组中删除该用户。

Memberof和refint叠加层

应启用 memberof 和 refint 叠加层。有关详细信息，请参见 "OpenLDAP 文档：Version 2.4 Administrator's Guide" 中的反向组成员资格维护说明。

索引

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，请确保用户名帮助中提到的字段已编入索引，以实现最佳性能。

请参见 "OpenLDAP 文档：Version 2.4 Administrator's Guide" 中有关反向组成员资格维护的信息。

管理 StorageGRID 中的管理员组

您可以创建管理员组来管理一个或多个管理员用户的安全权限。用户必须属于某个组，才能获得对 StorageGRID 系统的访问权限。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 如果您计划导入联合组，则表示您已配置身份联合，并且该联合组已存在于配置的身份源中。

创建管理员组

管理员组允许您确定哪些用户可以访问 Grid Manager 和 Grid Management API 中的哪些功能和操作。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 管理员组。
2. 选择*创建群组*。

选择组类型

您可以创建本地组或导入联合组。

- 如果要将权限分配给本地用户，请创建本地组。
- 创建联合组以从身份源导入用户。

本地组

步骤

1. 选择*本地组*。
2. 输入组的显示名称，您可以稍后根据需要进行更新。例如，"Maintenance Users"或"ILM Administrators"。
3. 请输入该组的唯一名称，您以后无法更新该名称。
4. 选择 **Continue**。

联合组

步骤

1. 选择*联合组*。
2. 输入要导入的组的名称，与配置的身份源中显示的名称完全相同。
   - 对于 Active Directory 和 Microsoft Entra ID，请使用 sAMAccountName。
   - 对于 OpenLDAP，请使用 CN（通用名称）。
   - 对于其他 LDAP，请使用 LDAP 服务器的适当唯一名称。
3. 选择 **Continue**。

管理组权限

步骤

1. 对于*访问模式*，选择组中的用户是否可以在 Grid Manager 和 Grid Management API 中更改设置和执行操作，或者他们是否只能查看设置和功能。
   - 读写（默认）：用户可以更改设置并执行其管理权限允许的操作。
   - 只读：用户只能查看设置和功能。他们无法在 Grid Manager 或 Grid Management 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，且任何组设置为*只读*，则该用户将对所有选定设置和功能具有只读访问权限。

2. 选择一个或多个 "管理员组权限"。

   您必须为每个组分配至少一个权限；否则，属于该组的用户将无法登录 StorageGRID。

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

添加用户（仅限本地组）

步骤

1. 可选地，为此组选择一个或多个本地用户。

   如果您尚未创建本地用户，则可以在不添加用户的情况下保存组。您可以在"用户"页面上将此组添加到用户。有关详细信息，请参阅 "管理用户"。

2. 选择*创建群组*并*完成*。

查看和编辑管理员组

您可以查看现有组的详细信息、修改组或复制组。

- 要查看所有组的基本信息，请查看"组"页面上的表格。
- 要查看特定组的所有详细信息或编辑组，请使用*操作*菜单或详细信息页面。

任务	**${post_edited_translations.segment}**	详细信息页面
查看群组详细信息	a. 选中该组的复选框。 b. 选择*操作* > 查看群组详细信息。	在表中选择组名称。
编辑显示名称（仅限本地组）	a. 选中该组的复选框。 b. 选择*操作* > 编辑组名称。 c. 输入新名称。 d. 选择 **Save changes**。	a. 选择组名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 **Save changes**。
编辑访问模式或权限	a. 选中该组的复选框。 b. 选择*操作* > 查看群组详细信息。 c. （可选）更改组的访问模式。 d. （可选）选择或清除 "管理员组权限"。 e. 选择 **Save changes**。	a. 选择组名称以显示详细信息。 b. （可选）更改组的访问模式。 c. （可选）选择或清除 "管理员组权限"。 d. 选择 **Save changes**。

复制组

步骤

1. 选中该组的复选框。

2. 选择*操作* > 复制组。
3. 完成复制组向导。

删除组

当要从系统中删除该组时，可以删除管理组，并删除与该组关联的所有权限。删除管理组会从组中删除任何用户，但不会删除用户。

步骤

1. 在"组"页面中，选中要删除的每个组的复选框。
2. 选择*操作* > 删除组。
3. 选择*删除组*。

StorageGRID 中的管理组权限

在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 Grid Manager 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此类管理员组，以确定该用户可以执行的任务。

必须为每个组分配至少一个权限；否则，属于该组的用户将无法登录到 Grid Manager 或 Grid Management API。

默认情况下，属于至少具有一个权限的组的任何用户都可以执行以下任务：

- 登录到网格管理器
- 查看控制面板
- 查看节点页面
- ${post_edited_translations.segment}
- 更改自己的密码（仅限本地用户）
- 查看配置和维护页面上提供的某些信息

${post_edited_translations.segment}

对于所有权限，组的“访问模式”设置决定了用户是可以更改设置并执行操作，还是只能查看相关设置和功能。如果一个用户属于多个组，且其中任何一个组被设置为“只读”，则该用户对所有选定的设置和功能将具有只读访问权限。

以下各节介绍了创建或编辑管理员组时可以分配的权限。任何未明确提及的功能都需要 **Root access** 权限。

Root 访问

此权限提供对所有网格管理功能的访问。

更改租户 root 密码

此权限提供对租户页面上的*更改根密码*选项的访问权限，允许您控制谁可以更改租户的本地 root 用户的密码。启用 S3 密钥导入功能时，此权限也用于迁移 S3 密钥。没有此权限的用户无法看到*更改根密码*选项。

要授予对包含*更改 root 密码*选项的租户页面的访问权限，还应分配*租户帐户*权限。

ILM

此权限提供对以下 **ILM** 菜单选项的访问权限：

- 规则
- 策略
- 策略标签
- 存储池
- 存储级别
- 地区
- 对象元数据查找

用户必须具有*其他网格配置*权限才能管理存储等级。

维护

用户必须具有维护权限才能使用这些选项：

- 配置 > 访问控制：
  - 网格密码
- 配置 > 网络：
  - S3端点域名
- 维护 > 任务：
  - 停用
  - 扩展
  - 对象存在性检查
  - 恢复
- 维护 > 系统：
  - 恢复包
  - 软件更新
- 支持 > 工具：
  - 日志

${post_edited_translations.segment}

- 维护 > 网络：
  - DNS 服务器
  - 网格网络
  - NTP 服务器
- 维护 > 系统：
  - 许可证
- 配置 > 网络：
  - S3端点域名
- 配置 > 安全：
  - 证书
- 配置 > 监控：
  - 审核和 syslog 服务器

${post_edited_translations.segment}

此权限允许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默、警报通知和警报规则。

指标查询

此权限提供对以下内容的访问权限：

- ${post_edited_translations.segment}
- 使用网格管理 API 的 **Metrics** 部分自定义 Prometheus 指标查询
- 包含指标的 Grid Manager 仪表板卡片

对象元数据查找

此权限提供对 **ILM** > 对象元数据查找 页面的访问权限。

其他网格配置

此权限提供对以下附加网格配置选项的访问权限：

- **ILM**：
  - 存储级别
- 配置 > 系统：
- 支持 > 其他：
  - 链路成本

存储设备管理员

此权限提供：

- 通过 Grid Manager 访问存储设备上的 E 系列 SANtricity System Manager。
- 能够在支持这些操作的设备的"管理驱动器"选项卡上执行故障排除和维护任务。

租户帐户

此权限允许：

- 访问租户页面，您可以在其中创建、编辑和删除租户帐户
- 查看现有流量分类策略
- 查看包含租户详细信息的网格管理器仪表板卡片

在 StorageGRID 中管理用户

您可以查看本地用户和联合用户。您还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 Grid Manager 功能。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

创建本地用户

您可以创建一个或多个本地用户，并将每个用户分配到一个或多个本地组。组的权限控制用户可以访问的 Grid Manager 和 Grid Management API 功能。

您只能创建本地用户。使用外部身份源管理联合用户和组。

网格管理器包括一个名为"root"的预定义本地用户。您无法删除 root 用户。

> 如果启用了单一登录 (SSO)，则本地用户无法登录到 StorageGRID。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 管理员用户。
2. 选择*创建用户*。

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}
2. （可选）如果此用户无权访问 Grid Manager 或 Grid Management API，请选择 **Yes**。
3. 选择 **Continue**。

分配到组

步骤

1. ${post_edited_translations.segment}

   如果您尚未创建组，则可以在不选择组的情况下保存该用户。您可以在“组”页面上将此用户添加到组中。

   如果用户属于多个组，则权限是累积的。请参见 "管理管理员组" 了解详细信息。

2. 选择*创建用户*并选择*完成*。

${post_edited_translations.segment}

您可以查看现有本地用户和联合用户的详细信息。您可以修改本地用户，以更改该用户的全名、密码或组群成员身份。您还可以临时阻止用户访问 Grid Manager 和 Grid Management API。

您只能编辑本地用户。请使用外部身份源来管理联合用户。

- 若要查看所有本地和联合用户的基本信息，请查看"用户"页面上的表。
- ${post_edited_translations.segment}

  ${post_edited_translations.segment}

  ${post_edited_translations.segment}

任务	**${post_edited_translations.segment}**	详细信息页面
${post_edited_translations.segment}	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment}	在表中选择用户的名称。
编辑全名（仅限本地用户）	a. ${post_edited_translations.segment} b. 选择*操作* > 编辑全名。 c. 输入新名称。 d. 选择 **Save changes**。	a. 选择用户名以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 **Save changes**。
拒绝或允许 StorageGRID 访问	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. 选择 Access 选项卡。 d. ${post_edited_translations.segment} e. 选择 **Save changes**。	a. 选择用户名以显示详细信息。 b. 选择 Access 选项卡。 c. ${post_edited_translations.segment} d. 选择 **Save changes**。

任务	**${post_edited_translations.segment}**	详细信息页面
${post_edited_translations.segment}	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. 选择"密码"选项卡。 d. ${post_edited_translations.segment} e. 选择*更改密码*。	a. 选择用户名以显示详细信息。 b. 选择"密码"选项卡。 c. ${post_edited_translations.segment} d. 选择*更改密码*。
${post_edited_translations.segment}	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. ${post_edited_translations.segment} e. 选择*Edit groups*以选择不同的群组。 f. 选择 **Save changes**。	a. 选择用户名以显示详细信息。 b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. 选择*Edit groups*以选择不同的群组。 e. 选择 **Save changes**。

导入联合用户

${post_edited_translations.segment}

步骤

1. 选择*配置* > 访问控制 > 管理员用户。
2. ${post_edited_translations.segment}
3. 输入一个或多个联合用户的 UUID 或用户名。

   对于多个条目，请在新行中添加每个 UUID 或用户名。

4. 选择*导入*。

   如果一个或多个用户的"用户"字段导入失败，请执行以下步骤：

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 完成复制用户向导。

删除用户

${post_edited_translations.segment}

> 您无法删除 root 用户。

步骤

1. ${post_edited_translations.segment}
2. 选择*操作* > 删除用户。
3. ${post_edited_translations.segment}

使用单点登录 (SSO)

了解 StorageGRID SSO

启用单点登录(SSO)后，只有在使用组织实施的SSO登录过程对其凭据进行授权的情况下，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。本地用户无法登录StorageGRID。

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)。

在启用单点登录 (SSO) 之前，请查看启用 SSO 时 StorageGRID 登录和注销流程如何受到影响。

启用 SSO 时登录

启用 SSO 并登录 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。

   - 如果这是您第一次在此浏览器上访问该 URL，系统会提示您输入帐户 ID。
   - 如果您以前访问过 Grid Manager 或 Tenant Manager，系统会提示您选择最近的帐户或输入帐户 ID。

   > 当您输入租户帐户的完整 URL（即，完全限定的域名或 IP 地址，后跟 `/?accountId=20-digit-account-id`）时，不会显示 StorageGRID 登录页面。相反，系统会立即将您重定向到组织的 SSO 登录页面，您可以在此处 使用 SSO 凭据登录。

2. 指示是要访问网格管理器还是租户管理器：
   - 要访问 Grid Manager，请将 **Account ID** 字段留空，输入 **0** 作为帐户 ID，或者在最近的帐户列表中显示时选择 **Grid Manager**。
   - 要访问租户管理器，请输入 20 位租户帐户 ID，或者按名称选择一个租户（如果它显示在最近的帐户列表中）。
3. 选择*登录*

StorageGRID 将您重定向到组织的 SSO 登录页面。例如：

4. 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) 向 StorageGRID 提供身份验证响应。
   b. StorageGRID 验证身份验证响应。
   c. 如果响应有效，并且您属于具有 StorageGRID 访问权限的联合组，则您将登录到 Grid Manager 或 Tenant Manager，具体取决于您选择的帐户。

   > 如果无法访问服务帐户，只要您是属于具有 StorageGRID 访问权限的联合组的现有用户，您仍然可以登录。

5. 如果您有足够的权限，也可以选择访问其他管理节点，或访问 Grid Manager 或 Tenant Manager。

   您无需重新输入 SSO 凭据。

启用 **SSO** 时注销

为 StorageGRID 启用 SSO 后，注销时会发生什么情况取决于您登录的内容和注销位置。

步骤

1. 在用户界面的右上角找到*注销*链接。
2. 选择*退出*。

   此时将显示 StorageGRID 登录页面。最近的帐户*下拉列表已更新，包括 ***Grid Manager** 或租户的名称，以便将来可以更快地访问这些用户界面。

> 下表汇总了使用单个浏览器会话时注销会发生的情况。如果您已跨多个浏览器会话登录 StorageGRID，则必须分别从所有浏览器会话中注销。

如果您已登录到……	然后您退出……	您已退出……
一个或多个管理节点上的 Grid Manager	任何管理节点上的 Grid Manager	所有管理节点上的 Grid Manager 注意： 如果您将 Entra ID 用于 SSO，则可能需要几分钟时间才能从所有管理节点中注销。
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	Grid Manager	仅网格管理器。您还必须注销租户管理器才能注销 SSO。

StorageGRID SSO 的要求和注意事项

在为 StorageGRID 系统启用单点登录 (SSO) 之前，请查看要求和注意事项。

${post_edited_translations.segment}

${post_edited_translations.segment}

- Active Directory 联合身份验证服务 (AD FS)
- ${post_edited_translations.segment}
- PingFederate

您必须先为 StorageGRID 系统配置身份联合，然后才能配置 SSO 身份提供程序。用于身份联合的 LDAP 服务类型决定了您可以实施的 SSO 类型。

已配置的**LDAP**服务类型	**SSO** 身份提供程序的选项
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

AD FS 要求

您可以使用以下任一版本的 AD FS：

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

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

其他要求

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

Entra ID 注意事项

如果使用 Entra ID 作为 SSO 类型，并且用户的用户主体名称不使用 sAMAccountName 作为前缀，则当 StorageGRID 与 LDAP 服务器断开连接时，可能会出现登录问题。若要允许用户登录，必须还原与 LDAP 服务器的连接。

服务器证书要求

默认情况下，StorageGRID 在每个管理节点上使用管理接口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。当您为 StorageGRID 配置信赖方信任（AD FS）、企业应用程序（Entra ID）或

服务提供商连接（PingFederate）时，将使用服务器证书作为 StorageGRID 请求的签名证书。

如果您还没有"已为管理界面配置自定义证书"，现在应该执行此操作。安装自定义服务器证书时，它将用于所有管理节点，并且可以在所有 StorageGRID 依赖方信任、企业应用程序或 SP 连接中使用。

> 不建议在依赖方信任、企业应用程序或 SP 连接中使用管理节点的默认服务器证书。如果节点出现故障并恢复，则会生成一个新的默认服务器证书。在登录到恢复的节点之前，您必须使用新证书更新依赖方信任、企业应用程序或 SP 连接。

您可以通过登录到节点的命令 shell 并转到 `/var/local/mgmt-api`目录来访问管理节点的服务器证书。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`。

端口要求

单点登录 (SSO) 在受限 Grid Manager 或 Tenant Manager 端口上不可用。如果希望用户使用单点登录进行身份验证，则必须使用默认 HTTPS 端口 (443)。请参阅 "控制外部防火墙的访问"。

确认联合用户可以登录到 StorageGRID

在启用单点登录 (SSO) 之前，必须确认至少有一个联合用户可以登录到 Grid Manager 以及任何现有租户帐户的 Tenant Manager。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 您已配置身份联盟。

步骤

1. 如果存在现有租户帐户，请确认没有任何租户正在使用自己的身份源。

   > 启用 SSO 时，租户管理器中配置的身份源将被 Grid Manager 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 Grid Manager 身份源的帐户。

   a. 登录到每个租户帐户的 Tenant Manager。
   b. 选择*访问管理* > 身份联合。
   c. 确认未选中*启用身份联合*复选框。
   d. 如果是，请确认不再需要用于此租户帐户的任何联合组，清除复选框，然后选择 **Save**。

2. 确认联合用户可以访问 Grid Manager：
   a. 在 Grid Manager 中，选择 **Configuration** > **Access control** > **Admin groups**。
   b. 请确保已从 Active Directory 身份源导入至少一个联合组，并且已为其分配了 Root 访问权限。
   c. 注销。
   d. 确认您可以作为联合组中的用户重新登录到 Grid Manager。

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，然后选择*操作* > 编辑。
c. 在"输入详细信息"选项卡上，选择 **Continue**。
d. 如果选中*使用自己的身份源*复选框，请取消选中该复选框并选择*保存*。

   此时将显示租户页面。

e. 选择租户帐户，选择*登录*，然后以本地 root 用户身份登录到租户帐户。
f. 在租户管理器中，选择*访问管理* > 组。
g. 请确保来自 Grid Manager 的至少一个联合组已为此租户分配了 Root 访问权限。
h. 注销。
i. 确认可以作为联合组中的用户重新登录到租户。

相关信息

- "单点登录的要求和注意事项"
- "管理管理员组"
- "使用租户帐户"

在 StorageGRID 中配置 SSO

您可以按照配置 SSO 向导并进入沙盒模式来配置和测试单点登录 (SSO)，然后再为所有 StorageGRID 用户启用它。启用 SSO 后，您可以在需要更改或重新测试配置时返回沙盒模式。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。
- 您已为 StorageGRID 系统配置身份联合。
- 对于身份联合 **LDAP** 服务类型，已根据计划使用的 SSO 身份提供程序选择 Active Directory 或 Entra ID。

已配置的**LDAP**服务类型	**SSO** 身份提供程序的选项
Active Directory 联合身份验证服务 (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

关于此任务

启用 SSO 并且用户尝试登录管理节点时，StorageGRID 将向 SSO 身份提供程序发送身份验证请求。反过来，SSO 身份提供程序将向 StorageGRID 发回身份验证响应，指示身份验证请求是否成功。对于成功的请求：

- Active Directory 或 PingFederate 的响应中包含该用户的通用唯一标识符 (UUID)。
- 来自 Entra ID 的响应包括用户主体名称 (UPN)。

${post_edited_translations.segment}

1. 在 StorageGRID 中配置设置。
2. 使用 SSO 身份提供程序的软件为每个管理节点创建信赖方信任 (AD FS)、企业应用程序 (Entra ID) 或服务提供商 (PingFederate)。
3. 返回 StorageGRID 以启用 SSO。

沙箱模式便于您进行这种反复配置，并在启用 SSO 之前测试所有设置。在使用沙箱模式时，用户无法使用 SSO 登录。

访问此向导

步骤

1. 选择 配置 > 访问控制 > 单点登录。此时将显示“单点登录”页面。

   如果禁用了"配置 SSO 设置"按钮，请确认已将身份提供程序配置为联合身份源。请参阅 "单点登录的要求和注意事项"。

2. 选择*配置 SSO 设置*。此时将显示提供标识提供程序详细信息页面。

提供标识提供程序详细信息

步骤

1. 从下拉列表中选择 **SSO** 类型。
2. 如果选择 Active Directory 作为 SSO 类型，请输入身份提供程序的*联合身份验证服务名称*，与 Active Directory 联合身份验证服务 (AD FS) 中显示的完全相同。

   要查找联合身份验证服务名称，请转到 Windows Server Manager。选择 **Tools** > **AD FS Management**。从操作菜单中，选择 **Edit Federation Service Properties**。联合身份验证服务名称显示在第二个字段中。

3. 指定当身份提供商响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接。
   - **Use operating system CA certificate**：使用操作系统上安装的默认 CA 证书来保护连接。
   - 使用自定义 **CA** 证书：使用自定义 CA 证书来保护连接。

     如果选择此设置，请复制自定义证书的文本，并将其粘贴到 **CA Certificate** 文本框中。

   - 不使用 **TLS**：不使用 TLS 证书来保护连接。

     如果更改 CA 证书，请立即 "在 Admin Nodes 上重新启动 mgmt-api 服务" 并测试是否能成功登录 Grid Manager。

4. 选择*继续*。此时将显示"提供信赖方标识符"页面。

提供依赖方标识符

1. 根据您选择的 SSO 类型，填写"提供信赖方标识符"页面上的字段。

Active Directory

a. 指定 StorageGRID 的*依赖方标识符*。此值控制您在 AD FS 中为每个依赖方信任使用的名称。

   - 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`。
   - 如果您的网格包含多个管理节点，请在标识符中包含字符串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字符串后，系统将生成一个表，根据节点的主机名显示网格中每个管理节点的依赖方标识符。

   > 您必须为 StorageGRID 系统中的每个管理节点创建一个依赖方信任。为每个管理节点创建依赖方信任可确保用户能够安全地登录和退出任何管理节点。

b. 选择*保存并进入沙盒模式*。

Entra ID

a. 在企业应用程序部分，为 StorageGRID 指定*企业应用程序名称*。此值控制您在 Entra ID 中为每个企业应用程序使用的名称。

   - 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，请在标识符中包含字符串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字符串后，系统将生成一个表，根据节点的主机名显示系统中每个管理节点的企业应用程序名称。

   > 您必须为 StorageGRID 系统中的每个管理节点创建一个企业应用程序。为每个管理节点提供企业应用程序可确保用户可以安全地登录和退出任何管理节点。

b. 按照"在 Entra ID 中创建企业应用程序"中的步骤为表中列出的每个管理节点创建企业应用程序。

c. 从 Entra ID 复制每个企业应用程序的联合元数据 URL。然后，将此 URL 粘贴到 StorageGRID 中对应的*联合元数据 URL* 字段中。

d. 复制并粘贴所有管理节点的联合元数据 URL 后，请选择*保存并进入沙盒模式*。

PingFederate

a. 在服务提供商 (SP) 部分，指定 StorageGRID 的 **SP** 连接 **ID**。此值控制您在 PingFederate 中为每个 SP 连接使用的名称。

   - 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`。
   - 如果您的网格包含多个管理节点，请在标识符中包含字符串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字符串后，系统将生成一个表，根据节点的主机名显示系统中每个管理节点的 SP 连接 ID。

   > 您必须为 StorageGRID 系统中的每个管理节点创建 SP 连接。为每个管理节点建立 SP 连接可确保用户能够安全地登录和退出任何管理节点。

b. 在*联合元数据 URL* 字段中为每个管理节点指定联合元数据 URL。

   使用以下格式：

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

c. 选择*保存并进入沙盒模式*。

配置依赖方信任、企业应用程序或 **SP** 连接

保存配置并进入沙盒模式后，您可以完成并测试所选 SSO 类型的配置。

StorageGRID 可以根据需要保持沙盒模式。但是，只有联合用户和本地用户才能登录。

Active Directory

步骤

1. 转至 Active Directory Federation Services (AD FS)。
2. 使用"配置 SSO"页面上表格中显示的每个依赖方标识符，为 StorageGRID 创建一个或多个依赖方信任。

   必须为表中显示的每个管理节点创建一个信任。

   有关说明，请转到 "在 AD FS 中创建依赖方信任"。

Entra ID

步骤

1. 从当前登录的管理节点的单一登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到该节点。
   b. 选择*配置* > 访问控制 > 单点登录。
   c. 下载并保存该节点的 SAML 元数据。
3. 转到 Azure 门户。
4. 按照 "在 Entra ID 中创建企业应用程序" 中的步骤，将每个管理节点的 SAML 元数据文件上传到其相应的 Entra ID 企业应用程序中。

PingFederate

步骤

1. 从当前登录的管理节点的单一登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到该节点。
   b. 选择*配置* > 访问控制 > 单点登录。
   c. 下载并保存该节点的 SAML 元数据。
3. 转至 PingFederate。
4. "为 StorageGRID 创建一个或多个服务提供商 (SP) 连接"。使用每个管理节点的 SP 连接 ID（显示在配置 SSO 页面上的表格中）以及为该管理节点下载的 SAML 元数据。

   您必须为表中显示的每个管理节点创建一个 SP 连接。

测试配置

在对整个 StorageGRID 系统强制使用单点登录之前，请确认已为每个管理节点正确配置了单点登录和单点注销。

Active Directory

步骤

1. 在 Configure SSO 页面中，找到向导 Test configuration 步骤中的链接。

   URL 派生自您在 **Federation service name** 字段中输入的值。

2. 选择链接，或将 URL 复制并粘贴到浏览器中，以访问身份提供商的登录页面。
3. 要确认您可以使用 SSO 登录 StorageGRID，请选择 登录以下站点之一，为主管理节点选择依赖方标识符，然后选择 登录。
4. 请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 操作不成功，系统将显示一条错误消息。请修复该问题，清除浏览器的 Cookie，然后重试。
5. 重复这些步骤以验证网格中每个管理节点的 SSO 连接。

Entra ID

步骤

1. 转到 Azure 门户中的"单一登录"页面。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   - 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 操作不成功，系统将显示一条错误消息。请修复该问题，清除浏览器的 Cookie，然后重试。
4. 重复这些步骤以验证网格中每个管理节点的 SSO 连接。

PingFederate

步骤

1. ${post_edited_translations.segment}

   一次选择并测试一个链接。

2. ${post_edited_translations.segment}
   - 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 操作不成功，系统将显示一条错误消息。请修复该问题，清除浏览器的 Cookie，然后重试。
3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

启用单点登录

确认可以使用 SSO 登录每个管理节点后，就可以为整个 StorageGRID 系统启用 SSO。

启用 SSO 后，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。

步骤

1. 从配置 SSO 向导的测试配置步骤中，选择 **Enable SSO**。
2. 查看警告消息，然后选择*启用 SSO*。

   单点登录现已启用。此时将显示单一登录页面，其中包含刚刚配置的 SSO 的详细信息。

3. 要编辑配置，请选择*编辑*。
4. 要禁用单点登录，请选择 **Disable SSO**。

如果您使用 Azure 门户，并且从用于访问 Entra ID 的同一台计算机访问 StorageGRID，请确保 Azure 门户用户也是已授权的 StorageGRID 用户（已导入到 StorageGRID 的联合组中的用户），或者在尝试登录 StorageGRID 之前先退出 Azure 门户。

在 **AD FS** 中为 **StorageGRID** 创建信赖方信任

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。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择 **AD FS** 作为 SSO 类型。
- 您已在 Grid Manager 中拥有"已进入沙盒模式"。
- 您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。您可以在 StorageGRID 配置 SSO 页面上的管理节点详细信息表中找到这些值。

  您必须为 StorageGRID 系统中的每个管理节点创建一个依赖方信任。为每个管理节点创建依赖方信任可确保用户能够安全地登录和退出任何管理节点。

- 您具有在 AD FS 中创建依赖方信任的经验，或者您具有 Microsoft AD FS 文档的访问权限。
- 您正在使用 AD FS Management 管理单元，并且您属于 Administrators 组。
- 如果要手动创建依赖方信任，则具有为 StorageGRID 管理界面上传的自定义证书，或者您知道如何从命令 Shell 登录到管理节点。

关于此任务

这些说明适用于 Windows Server 2016 AD FS。如果使用的是不同版本的 AD FS，您会注意到操作过程中的细微差异。如果有疑问，请参阅 Microsoft AD FS 文档。

使用 **Windows PowerShell** 创建信赖方信任

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

步骤

1. 从 Windows "开始"菜单中，右键选择 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"
   ```

   - 对于 *Admin_Node_Identifier*，请输入管理节点的信赖方标识符，与单一登录页面上显示的完全相同。例如， `SG-DC1-ADM1`。
   - 对于 *Admin_Node_FQDN*，请为同一个管理节点输入完全限定的域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）
3. 从 Windows Server Manager 中，选择 **Tools** > **AD FS Management**。

   此时将显示AD FS管理工具。
4. 选择 **AD FS** > **Relying Party Trusts**。

   此时将显示依赖方信任列表。
5. 将访问控制策略添加到新创建的依赖方信任：
   a. 找到您刚刚创建的信赖方信任。
   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. 选择 **Apply**，然后选择 **OK**
6. 将声明颁发策略添加到新创建的信赖方信任：
   a. 找到您刚刚创建的信赖方信任。
   b. 右键单击信任，然后选择 **Edit claim issuance policy**。
   c. 选择*添加规则*。
   d. 在"选择规则模板"页面上，从列表中选择*Send LDAP Attributes as Claims*，然后选择*Next*。
   e. 在"配置规则"页面上，输入此规则的显示名称。

      例如，**ObjectGUID to Name ID** 或 **UPN to Name ID**。
   f. 对于属性存储，选择 **Active Directory**。
   g. 在 Mapping 表的 LDAP Attribute 列中，键入 **objectGUID** 或选择 **User-Principal-Name**。
   h. 在 Mapping 表的 Outgoing Claim Type 列中，从下拉列表中选择 **Name ID**。
   i. 选择*完成*，然后选择*确定*。
7. 确认已成功导入元数据。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认*端点*、*标识符*和*签名*选项卡上的字段已填充。

      如果缺少元数据，请确认联合元数据地址正确，或手动输入值。

8. 重复这些步骤，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 StorageGRID 并 "测试所有依赖方信任" 以确认它们配置正确。

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。

步骤

1. 在 Windows Server Manager 中，选择*工具*，然后选择 **AD FS Management**。
2. 在操作下方，选择*添加信赖方信任*。
3. 在欢迎页面上，选择 **Claims aware**，然后选择 **Start**。
4. 选择*导入有关在线或本地网络上发布的依赖方的数据*。
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`

   对于 *Admin_Node_FQDN*，请为同一个管理节点输入完全限定的域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）

6. 完成信赖方信任向导，保存信赖方信任，然后关闭此向导。

   输入显示名称时，请使用管理节点的信赖方标识符，与 Grid Manager 中单点登录页面上显示的完全相同。例如， `SG-DC1-ADM1`。

7. 添加声明规则：
   a. 右键单击信任，然后选择 **Edit claim issuance policy**。
   b. 选择*添加规则*：
   c. 在"选择规则模板"页面上，从列表中选择*Send LDAP Attributes as Claims*，然后选择*Next*。
   d. 在"配置规则"页面上，输入此规则的显示名称。

      例如，**ObjectGUID to Name ID** 或 **UPN to Name ID**。

   e. 对于属性存储，选择 **Active Directory**。
   f. 在 Mapping 表的 LDAP Attribute 列中，键入 **objectGUID** 或选择 **User-Principal-Name**。
   g. 在 Mapping 表的 Outgoing Claim Type 列中，从下拉列表中选择 **Name ID**。
   h. 选择*完成*，然后选择*确定*。
8. 确认已成功导入元数据。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认*端点*、*标识符*和*签名*选项卡上的字段已填充。

      如果缺少元数据，请确认联合元数据地址正确，或手动输入值。

9. 重复这些步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。
10. 完成后，请返回 StorageGRID 并 "测试所有依赖方信任" 以确认它们配置正确。

手动创建依赖方信任

如果选择不导入依赖部件信任的数据，则可以手动输入值。

步骤

1. 在 Windows Server Manager 中，选择*工具*，然后选择 **AD FS Management**。
2. 在操作下方，选择*添加信赖方信任*。
3. 在欢迎页面上，选择 **Claims aware**，然后选择 **Start**。
4. 选择*手动输入有关依赖方的数据*，然后选择*下一步*。
5. 完成信赖方信任向导：

   a. 输入此管理节点的显示名称。

      为了保持一致性，请使用管理节点的信赖方标识符，与 Grid Manager 中"单点登录"页面上的标识符完全相同。例如， `SG-DC1-ADM1`。

   b. 跳过此步骤以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`

      对于 *`Admin_Node_FQDN`*，请输入管理节点的完全限定域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）

   e. 在"配置标识符"页面上，为同一管理节点指定信赖方标识符：

      `Admin_Node_Identifier`

      对于 *`Admin_Node_Identifier`*，请输入管理节点的信赖方标识符，与单一登录页面上显示的完全相同。例如， `SG-DC1-ADM1`。

   f. 检查设置，保存依赖方信任，然后关闭此向导。

      ${post_edited_translations.segment}

      如果未显示此对话框，请右键单击信任，然后选择*Edit claim issuance policy*。

6. 要启动声明规则向导，请选择*添加规则*：

   a. 在"选择规则模板"页面上，从列表中选择*Send LDAP Attributes as Claims*，然后选择*Next*。

   b. 在"配置规则"页面上，输入此规则的显示名称。

      例如，**ObjectGUID to Name ID** 或 **UPN to Name ID**。

c. 对于属性存储，选择 **Active Directory**。

d. 在 Mapping 表的 LDAP Attribute 列中，键入 **objectGUID** 或选择 **User-Principal-Name**。

e. 在 Mapping 表的 Outgoing Claim Type 列中，从下拉列表中选择 **Name ID**。

f. 选择*完成*，然后选择*确定*。

7. 右键单击依赖方信任以打开其属性。

8. 在 **Endpoints** 选项卡上，为单次注销 (SLO) 配置端点：

a. 选择 **Add SAML**。

b. 选择*端点类型* > **SAML** 注销。

c. 选择*绑定* > 重定向。

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

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

对于 *Admin_Node_FQDN*，请输入管理节点的完全限定域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）

a. 选择 **OK**。

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：

- 如果您有已上传到 StorageGRID 的自定义管理证书，请选择该证书。
- 如果没有自定义证书，请登录到管理节点，转到管理节点的 `/var/local/mgmt-api`目录，然后添加 `custom-server.crt`证书文件。

> 不建议使用管理节点的默认证书 (`server.crt`）。如果管理节点发生故障，则在恢复该节点时将重新生成默认证书，您需要更新依赖方信任。

b. 选择*应用*，然后选择*确定*。

已保存并关闭信赖方属性。

10. 重复这些步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

11. 完成后，请返回 StorageGRID 并 "测试所有依赖方信任" 以确认它们配置正确。

在 Entra ID 中为 StorageGRID 创建企业应用程序

您可以使用 Entra ID 为系统中的每个管理节点创建企业应用程序。

开始之前

- 您已开始为 StorageGRID 配置单点登录，并选择 **Entra ID** 作为 SSO 类型。
- 您在 Grid Manager 中拥有 "已进入沙盒模式"。
- 您拥有系统中每个管理节点的 **Enterprise application name**。您可以从配置 SSO 页面上的管理节点详细信

息表中复制这些值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个企业应用程序。为每个管理节点提供企业应用程序可确保用户可以安全地登录和退出任何管理节点。

- 您有在 Entra ID 中创建企业应用程序的经验。
- 您拥有一个具有有效订阅的 Entra ID 帐户。
- 您在 Entra ID 帐户中具有以下角色之一：Global Administrator、Cloud Application Administrator 、Application Administrator 或服务主体的所有者。

访问 **Entra ID**

步骤

1. 登录到 "Azure Portal"。
2. 导航到 "Entra ID"。
3. 选择 "企业应用程序"。

创建企业应用程序并保存 **StorageGRID SSO** 配置

要将 Entra ID 的 SSO 配置保存在 StorageGRID 中，您必须使用 Entra ID 为每个管理节点创建企业应用程序。您将从 Entra ID 复制联合元数据 URL，并将其粘贴到配置 SSO 页面上相应的*联合元数据 URL* 字段中。

步骤

1. 对每个管理节点重复以下步骤。
   a. 在 Entra ID Enterprise 应用程序窗格中，选择 **New application**。
   b. 选择*创建自己的应用程序*。
   c. 对于名称，请输入您从"配置 SSO"页面上的"管理节点详细信息"表中复制的*企业应用程序名称*。
   d. 保持选中*集成库中未找到的任何其他应用程序（非库）*单选按钮。
   e. 选择 **Create**。
   f. 选择 *2. 中的*开始*链接设置单点登录*框，或选择左边距中的*单点登录*链接。
   g. 选择 **SAML** 框。
   h. 复制*应用联合元数据网址*，您可以在*步骤 3 SAML 签名证书*下找到该网址。
   i. 转到"配置 SSO"页面，然后将 URL 粘贴到与您使用的*企业应用程序名称*对应的*联合元数据 URL* 字段中。
2. 为每个管理节点粘贴联合元数据 URL 并对 SSO 配置进行所有其他必要更改后，请在配置 SSO 页面上选择*保存*。

为每个管理节点下载 **SAML** 元数据

保存 SSO 配置后，您可以为 StorageGRID 系统中的每个管理节点下载 SAML 元数据文件。

步骤

1. 对每个管理节点重复这些步骤。

a. 从管理节点登录到 StorageGRID。
b. 选择*配置* > 访问控制 > 单点登录。
c. 选择该按钮以下载该管理节点的 SAML 元数据。
d. 保存文件，并将其上传到 Entra ID。

将 **SAML** 元数据上传到每个企业应用程序

为每个 StorageGRID 管理节点下载 SAML 元数据文件后，在 Entra ID 中执行以下步骤：

步骤

1. 返回 Azure 门户。
2. 对每个企业应用程序重复以下步骤：

> 您可能需要刷新"企业应用程序"页面才能查看以前在列表中添加的应用程序。

a. 转到企业应用程序的"属性"页面。
b. 将*需要分配*设置为*否*（除非您想单独配置分配）。
c. 转到"单一登录"页面。
d. 完成 SAML 配置。
e. 选择*上传元数据文件*按钮，然后选择您为相应管理节点下载的 SAML 元数据文件。
f. 文件加载后，选择 **Save**，然后选择 **X** 关闭窗格。您将返回到"使用 SAML 设置单点登录"页面。

3. "测试每个应用程序"。

在 **PingFederate** 中为 **StorageGRID** 创建服务提供商连接

使用 PingFederate 为系统中的每个管理节点创建服务提供商 (SP) 连接。为了加快此过程，您将从 StorageGRID 导入 SAML 元数据。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择 **Ping Federate** 作为 SSO 类型。
- 您在 Grid Manager 中拥有 "已进入沙盒模式"。
- 您拥有系统内每个管理节点的 **SP** 连接 **ID**。您可以在“配置 SSO”页面上的管理节点详细信息表中找到这些值。
- ${post_edited_translations.segment}
- 您有在 PingFederate 服务器中创建 SP 连接的经验。
- 您有 "${post_edited_translations.segment}" for PingFederate Server。PingFederate 文档提供了详细的分步说明和解释。
- 您有 "${post_edited_translations.segment}" for PingFederate Server。

关于此任务

这些说明概述了如何将 PingFederate Server 10.3 版本配置为 StorageGRID 的 SSO 提供程序。如果您使用的是其他版本的 PingFederate，则可能需要调整 these 说明。有关您所用版本的详细说明，请参阅 PingFederate

Server 文档。

在 **PingFederate** 中完成先决条件

在创建用于 StorageGRID 的 SP 连接之前，您必须完成 PingFederate 中的先决条件任务。在配置 SP 连接时，您将使用这些先决条件中的信息。

${post_edited_translations.segment}

如果尚未创建，请创建一个数据存储以将 PingFederate 连接到 AD FS LDAP 服务器。使用您在 StorageGRID 中 "${post_edited_translations.segment}" 时使用的值。

- 类型：目录 (LDAP)
- **LDAP Type**：Active Directory
- ${post_edited_translations.segment}

创建密码凭据验证器

如果尚未创建，请创建密码凭据验证器。

- 类型：LDAP 用户名密码凭据验证器
- 数据存储：选择您创建的数据存储。
- ${post_edited_translations.segment}
- 搜索过滤器: sAMAccountName=${username}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

如果尚未创建，请创建一个 IdP 适配器实例。

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. 选择您创建的 密码凭据验证器。
6. ${post_edited_translations.segment}
7. 选择 **Save**。

创建或导入签名证书

如果尚未创建或导入签名证书，请先执行此操作。

步骤

1. 转到 **Security** > **Signing & Decryption Keys & Certificates**。
2. 创建或导入签名证书。

在 **PingFederate** 中创建 **SP** 连接

在 PingFederate 中创建 SP 连接时，您需要导入从 StorageGRID 为管理节点下载的 SAML 元数据。元数据文件包含许多您需要的特定值。

必须为 StorageGRID 系统中的每个管理节点创建 SP 连接，以便用户可以安全地登录和退出任何节点。使用以下说明创建第一个 SP 连接。然后，转到<<${post_edited_translations.segment}>>以创建您需要的任何其他连接。

选择 **SP** 连接类型

步骤

1. 转到*应用程序* > 集成 > **SP Connections**。
2. 选择*创建连接*。
3. 选择*不要为此连接使用模板*。
4. 选择 **Browser SSO Profiles** 和 **SAML 2.0** 作为协议。

导入 **SP** 元数据

步骤

1. 在"导入元数据"选项卡上，选择*文件*。
2. 选择您从管理节点的"配置 SSO"页面下载的 SAML 元数据文件。
3. 查看元数据摘要以及"常规信息"选项卡上提供的信息。

   合作伙伴的实体 ID 和连接名称设置为 StorageGRID SP 连接 ID。（例如，10.96.105.200-DC1-ADM1-105-200）。基本 URL 是 StorageGRID 管理节点的 IP。

4. 选择 **Next**。

配置 **IdP** 浏览器 **SSO**

步骤

1. 在浏览器 SSO 选项卡中，选择 **Configure Browser SSO**。
2. 在 SAML 配置文件选项卡上，选择 **SP-initiated SSO**、**SP-initial SLO**、**IdP-initiated SSO** 和 **IdP-initiated SLO** 选项。
3. 选择 **Next**。
4. 在 Assertion Lifetime 选项卡上，不做任何更改。
5. 在断言创建选项卡上，选择*Configure Assertion Creation*。
   a. 在身份映射选项卡上，选择*Standard*。
   b. 在 Attribute Contract 选项卡上，使用 **SAML_SUBJECT** 作为 Attribute Contract 和导入的未指定名称格式。
6. 对于 Extend the Contract，选择 **Delete** 以删除未使用的 `urn:oid`。

映射适配器实例

步骤

1. ${post_edited_translations.segment}
2. 在适配器实例选项卡上，选择您创建的 适配器实例。
3. 在"映射方法"选项卡上，选择*从数据存储中检索其他属性*。
4. 在"属性源和用户查找"选项卡上，选择*添加属性源*。
5. 在"数据存储"选项卡上，提供说明并选择您添加的 数据存储。
6. 在"LDAP 目录搜索"选项卡上：
   - 输入 **Base DN**，它应与您在 StorageGRID 中为 LDAP 服务器输入的值完全匹配。
   - 对于搜索范围，选择*Subtree*。
   - 对于根对象类，搜索并添加以下任一属性：**objectGUID** 或 **userPrincipalName**。
7. 在 LDAP 二进制属性编码类型选项卡上，为 **objectGUID** 属性选择 **Base64**。
8. 在 LDAP 筛选器选项卡上，输入 **sAMAccountName=${username}**。
9. 在 Attribute Contract Fulfillment（属性合同履行）选项卡上，从 Source（来源）下拉菜单中选择 **LDAP**（属性），然后从 Value（值）下拉菜单中选择 **objectGUID** 或 **userPrincipalName**。
10. 查看并保存属性源。
11. 在 Failsave Attribute Source 选项卡上，选择 **Abort the SSO Transaction**。
12. 查看摘要并选择*完成*。
13. 选择*完成*。

配置协议设置

步骤

1. 在 **SP Connection** > **Browser SSO** > **Protocol Settings** 选项卡上，选择 **Configure Protocol Settings**。
2. 在 Assertion Consumer Service URL 选项卡上，接受从 StorageGRID SAML 元数据导入的默认值（绑定为 **POST**，端点 URL 为 `/api/saml-response`）。
3. 在 SLO Service URLs 选项卡上，接受从 StorageGRID SAML 元数据导入的默认值（绑定为 **REDIRECT**，端点 URL 为 `/api/saml-logout`。
4. 在 Allowable SAML Bindings 选项卡上，清除 **ARTIFACT** 和 **SOAP**。只需要 **POST** 和 **REDIRECT**。
5. 在 Signature Policy（签名策略）选项卡上，保留 **Require Authn Requests to be Signed**（要求对身份验证请求进行签名）和 **Always Sign Assertion**（始终对断言进行签名）复选框处于选中状态。
6. 在加密策略选项卡上，选择*None*。
7. 查看摘要并选择*完成*以保存协议设置。
8. 查看摘要并选择*完成*以保存浏览器 SSO 设置。

配置凭据

步骤

1. 在 SP Connection 选项卡中，选择 **Credentials**。

2. 在凭据选项卡中，选择 配置凭据。
3. 选择您创建或导入的 签名证书。
4. 选择*下一步*转到*管理签名验证设置*。
    a. 在信任模型选项卡上，选择*Unanchored*。
    b. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以复制第一个 SP 连接，以为网格中的每个管理节点创建所需的 SP 连接。您需要为每个副本上传新的元数据。

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 选择与管理节点对应的元数据文件：
    a. ${post_edited_translations.segment}
    b. ${post_edited_translations.segment}
    c. 选择 **Next**。
    d. 选择 **Save**。
4. 解决由于未使用的属性导致的错误：
    a. 选择新连接。
    b. 选择 **Configure Browser SSO > Configure Assertion Creation > Attribute Contract**。
    c. 删除 **urn:oid** 的条目。
    d. 选择 **Save**。

在 StorageGRID 中禁用 SSO

如果您不再需要使用单点登录 (SSO) 功能，可以将其禁用。您必须先禁用单点登录，然后才能禁用身份联合。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

步骤

1. 选择*配置* > 访问控制 > 单点登录。

    此时将显示单一登录页面。

2. 选择*禁用 SSO*。
3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

${post_edited_translations.segment}

暂时禁用和重新启用 **StorageGRID** 管理节点的 **SSO**

如果单点登录 (SSO) 系统发生故障，您可能无法登录 Grid Manager。在这种情况下，您可以临时禁用并重新启用一个管理节点的 SSO。要禁用并重新启用 SSO，您必须访问该节点的命令 shell。

开始之前

- 您有 "特定访问权限"。
- 您拥有 `Passwords.txt` 文件。
- ${post_edited_translations.segment}

关于此任务

在为一个管理节点禁用 SSO 后，您可以作为本地 root 用户登录到 Grid Manager。为了确保 StorageGRID 系统的安全，您必须在退出登录后立即使用该节点的命令 shell 在该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。Grid Manager 中“单点登录”页面上的 * 启用 SSO* 复选框仍保持选中状态，并且所有现有 SSO 设置都将保留，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 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。
2. 运行以下命令：`disable-saml`

   ${post_edited_translations.segment}
3. 确认您要禁用 SSO。

   ${post_edited_translations.segment}
4. 在 Web 浏览器中，访问同一管理节点上的 Grid Manager。

   ${post_edited_translations.segment}

5. 使用用户名 root 和本地 root 用户的密码登录。
6. 如果因需要更正 SSO 配置而暂时禁用 SSO：
   a. 选择*配置* > 访问控制 > 单点登录。
   b. 更改不正确或过期的 SSO 设置。
   c. 选择 **Save**。

      ${post_edited_translations.segment}
7. 如果由于其他原因需要访问 Grid Manager 而暂时禁用了 SSO：
   a. ${post_edited_translations.segment}
   b. 选择*注销*，然后关闭 Grid Manager。
   c. 在管理节点上重新启用 SSO。您可以执行以下步骤之一：
      - 运行以下命令： `enable-saml`

        ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   ◦ 重新启动网格节点： `reboot`
8. ${post_edited_translations.segment}
9. ${post_edited_translations.segment}