控制对 StorageGRID 的访问

StorageGRID 11.8

NetApp
March 19, 2024

目录

控制对 StorageGRID 的访问

控制StorageGRID 访问：概述

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。您也可以选择启用单点登录（ SSO ），创建客户端证书和更改网格密码。

控制对网格管理器的访问

您可以通过从身份联合服务导入组和用户或设置本地组和本地用户来确定谁可以访问网格管理器和网格管理 API 。

使用 "身份联合" 进行设置 "组" 和 "users" 速度更快、并且允许用户使用熟悉的凭据登录到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。

您可以通过分配不同的来确定每个用户可以执行哪些任务 "权限" 每个组。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可以执行维护任务。用户必须至少属于一个组才能访问系统。

您也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。

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 ）。你先请 "配置并启用SSO"，所有用户都必须先通过外部身份提供程序进行身份验证，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。

更改配置密码短语

许多安装和维护过程以及下载 StorageGRID 恢复软件包都需要配置密码短语。下载 StorageGRID 系统的网格拓扑信息和加密密钥备份时，也需要使用密码短语。您可以 "更改密码短语" 根据需要。

更改节点控制台密码

网格中的每个节点都有一个唯一的节点控制台密码、您需要使用SSH以"admin"身份登录到此节点、或者通过VM/物理控制台连接登录到root用户。您可以根据需要执行此操作 "更改节点控制台密码" 对于每个节点。

更改配置密码短语

使用此操作步骤 更改 StorageGRID 配置密码短语。恢复，扩展和维护过程需要密码短语。下载恢复软件包备份时也需要使用密码短语，其中包括网格拓扑信息，网格节点控制台密码以及 StorageGRID 系统的加密密钥。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有维护或 root 访问权限。
- 您具有当前配置密码短语。

关于此任务

许多安装和维护过程以及都需要配置密码短语 "正在下载恢复包"。配置密码短语未在中列出 `Passwords.txt` 文件请务必记录配置密码短语并将其保存在安全的位置。

步骤

1. 选择 * 配置 * > * 访问控制 * > * 网格密码 * 。
2. 在*更改配置密码短语*下，选择*进行更改*
3. 输入当前配置密码短语。
4. 输入新密码短语。密码短语必须至少包含 8 个字符，并且不能超过 32 个字符。密码短语区分大小写。
5. 将新配置密码短语存储在安全位置。安装，扩展和维护过程需要使用它。
6. 重新输入新密码短语，然后选择 * 保存 * 。

   配置密码短语更改完成后，系统将显示一个绿色的成功横幅。

7. 选择 * 恢复包 * 。
8. 输入新的配置密码短语以下载新的恢复软件包。

   更改配置密码短语后，您必须立即下载新的恢复软件包。通过恢复包文件，您可以在发生故障时还原系统。

更改节点控制台密码

网格中的每个节点都有一个唯一的节点控制台密码，您需要使用该密码登录到该节点。按照以下步骤更改网格中每个节点的每个唯一节点控制台密码。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "维护或root访问权限"。
- 您具有当前配置密码短语。

关于此任务

使用节点控制台密码通过SSH以"admin"身份登录到节点、或者通过VM/物理控制台连接登录到root用户。更改节点控制台密码过程会为网格中的每个节点创建新密码、并将这些密码存储在更新的中 `Passwords.txt` 文件。密码将在 Passwords.txt 文件的 Password 列中列出。

用于节点间通信的 SSH 密钥具有单独的 SSH 访问密码。此操作步骤 不会更改SSH访问密码。

访问向导

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*。

输入配置密码短语

步骤

1. 输入网格的配置密码短语。
2. 选择 * 继续 * 。

[[download-current]]下载当前恢复软件包

在更改节点控制台密码之前、请下载当前恢复软件包。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. 选择 * 下载恢复包 * 。
2. 复制恢复软件包文件 (`.zip`)连接到两个安全、安全和独立的位置。

   恢复软件包文件必须受到保护、因为它包含可用于从StorageGRID 系统获取数据的加密密钥和密码。

3. 选择 * 继续 * 。
4. 出现确认对话框时、如果您已准备好开始更改节点控制台密码、请选择*是*。

   此过程启动后、您无法取消。

更改节点控制台密码

当节点控制台密码过程启动时、将生成一个包含新密码的新恢复软件包。然后、在每个节点上更新密码。

步骤

1. 等待生成新的恢复软件包、这可能需要几分钟时间。
2. 选择 * 下载新恢复包 * 。
3. 下载完成后：

   a. 打开 `.zip` 文件

   b. 确认您可以访问内容、包括 `Passwords.txt` 文件、其中包含新的节点控制台密码。

   c. 复制新的恢复软件包文件 (`.zip`)连接到两个安全、安全和独立的位置。

      请勿覆盖旧恢复软件包。

恢复软件包文件必须受到保护、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. 选中此复选框以指示您已下载新的恢复软件包并验证其内容。
5. 选择*更改节点控制台密码*、然后等待所有节点使用新密码进行更新。这可能需要几分钟时间。

   如果所有节点的密码均已更改，则会显示一个绿色的成功横幅。继续执行下一步。

   如果更新过程中出现错误，则会显示一条横幅消息，列出无法更改密码的节点数。系统将在任何无法更改密码的节点上自动重试此过程。如果此过程结束时某些节点仍没有更改密码，则会显示 * 重试 * 按钮。

   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 * 。

   > 重试仅会更改先前尝试更改密码期间失败的节点上的节点控制台密码。

6. 更改所有节点的节点控制台密码后、请删除 您下载的第一个恢复软件包。
7. (可选)使用*恢复包*链接下载新恢复包的附加副本。

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 。

为 Grid Manager 配置身份联合

如果您希望在 Active Directory ， Azure Active Directory （ Azure AD ） ， OpenLDAP 或 Oracle Directory Server 等其他系统中管理管理管理组和用户，则可以在网格管理器中配置身份联合。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您正在使用 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

  > 如果要使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP ，则必须配置 OpenLDAP 服务器。请参见 配置 OpenLDAP 服务器的准则。
- 如果您计划启用单点登录（ SSO ），则已查看 "单点登录的要求和注意事项"。
- 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，则身份提供程序正在使用 TLS 1.2 或 1.3 。请参见 "支持传出 TLS 连接的密码"。

关于此任务

如果要从 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 等其他系统导入组，则可以为

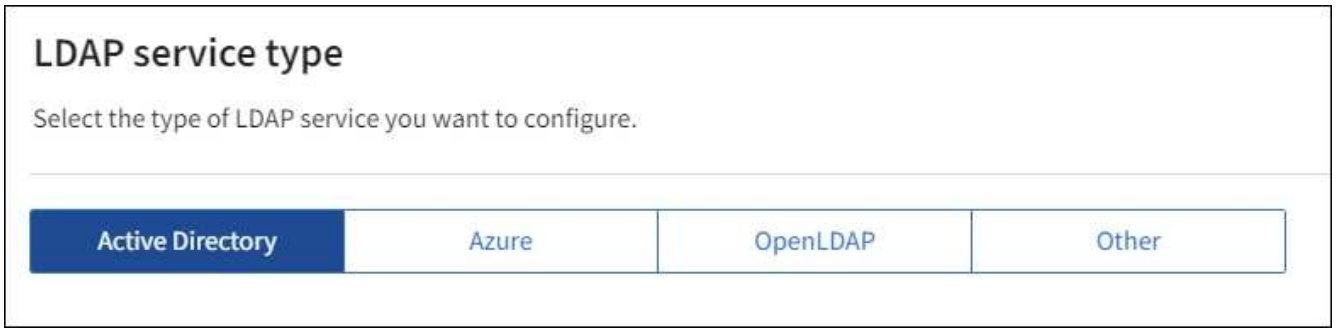
网格管理器配置身份源。您可以导入以下类型的组：

- 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。
- 不使用自己的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。请参见 "创建租户帐户" 和 "使用租户帐户" 了解详细信息。

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 服务类型部分中，选择要配置的 LDAP 服务类型。



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

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

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

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

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

指定的用户必须具有列出组和用户以及访问以下属性的权限：

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

◦ * 密码 * ：与用户名关联的密码。

> 如果您以后更改密码、则必须在此页面上更新密码。

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

> * 组唯一名称 * 值在其所属的 * 组基本 DN* 中必须是唯一的。

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

> 用户唯一名称 * 值在其所属的 * 用户基础 DN* 中必须是唯一的。

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

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

输入以下模式之一：

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

  与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。

◦ * 使用 STARTTLS * ：使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是建议的 Active Directory ， OpenLDAP 或其他选项，但 Azure 不支持此选项。

◦ * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。您必须为 Azure 选择此选项。

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

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

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

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

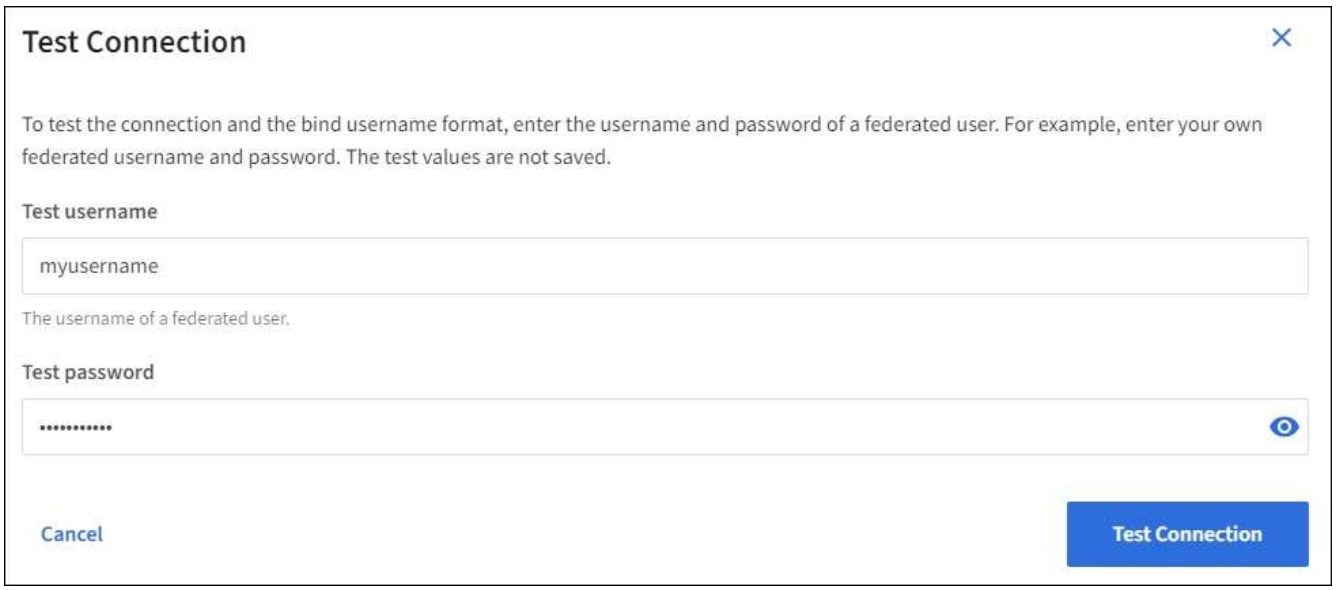
测试连接并保存配置

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

步骤

1. 选择 * 测试连接 * 。
2. 如果未提供绑定用户名格式：
   - 如果连接设置有效、则会显示"Test connection sule"(测试连接成功)消息。选择 * 保存 * 以保存配置。
   - 如果连接设置无效、则会显示"无法建立测试连接"消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。
3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

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



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

强制与身份源同步

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

步骤

1. 转到身份联合页面。
2. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

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

禁用身份联合

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

关于此任务

在禁用身份联合之前，您应注意以下事项：

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

步骤

1. 转到身份联合页面。
2. 取消选中*启用身份联合*复选框。

配置 OpenLDAP 服务器的准则

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

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

memberOf 和 fint 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明 "OpenLDAP 文档：版本 2.4 管理员指南"。

索引编制

您必须使用指定的索引关键字配置以下 OpenLDAP 属性：

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

此外，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息 "OpenLDAP 文档：版本 2.4 管理员指南"。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 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。

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。

访问向导

步骤

1. 选择 * 配置 * > * 访问控制 * > * 管理组 * 。
2. 选择 * 创建组 * 。

选择组类型

您可以创建本地组或导入联合组。

- 如果要为本地用户分配权限，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更新该名称。例如、"维护用户"或"ILM管理员"。
3. 输入组的唯一名称、此名称以后无法更新。
4. 选择 * 继续 * 。

联合组

步骤

1. 选择 * 联合组 * 。
2. 输入要导入的组的名称，与此名称在配置的身份源中显示的名称完全相同。
   - 对于 Active Directory 和 Azure ，请使用 sAMAccountName 。
   - 对于 OpenLDAP ，请使用 CN （公用名）。
   - 对于另一个 LDAP ，请为 LDAP 服务器使用适当的唯一名称。
3. 选择 * 继续 * 。

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。他们无法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。

2. 选择一个或多个 "管理员组权限"。

   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 。

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

添加用户（仅限本地组）

步骤

1. 或者，为此组选择一个或多个本地用户。

   如果尚未创建本地用户，则可以保存此组，而无需添加用户。您可以在用户页面上将此组添加到用户。请参见 "管理用户" 了解详细信息。

2. 选择 * 创建组 * 和 * 完成 * 。

查看和编辑管理组

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。
- 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	操作菜单	详细信息页面
查看组详细信息	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。	在表中选择组名称。
编辑显示名称（仅限本地组）	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 编辑组名称 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	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 * 保存更改 * 。
编辑访问模式或权限	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。 c. 也可以更改组的访问模式。 d. (可选)选择或清除 "管理员组权限"。 e. 选择 * 保存更改 * 。	a. 选择组名称以显示详细信息。 b. 也可以更改组的访问模式。 c. (可选)选择或清除 "管理员组权限"。 d. 选择 * 保存更改 * 。

复制组

步骤

1. 选中组对应的复选框。
2. 选择 * 操作 * > * 复制组 * 。
3. 完成复制组向导。

删除组

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。删除管理员组会从组中删除任何用户，但不会删除这些用户。

步骤

1. 在组页面中、选中要删除的每个组对应的复选框。
2. 选择 * 操作 * > * 删除组 * 。
3. 选择 * 删除组 * 。

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或网格管理 API 。

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）
- 查看配置和维护页面上提供的某些信息

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。

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具有 * 根访问权限 * 。

root 访问权限

通过此权限，可以访问所有网格管理功能。

确认警报（传统）

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。

更改租户 root 密码

通过此权限，您可以访问租户页面上的 * 更改 root 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。启用 S3 密钥导入功能后，此权限也用于迁移 S3 密钥。没有此权限的用户看不到*更改root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，还需要分配 * 租户帐户 * 权限。

网格拓扑页面配置

通过此权限，您可以访问 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的配置选项卡。

ILM

通过此权限，您可以访问以下 * ILM * 菜单选项：

- rules
- 策略
- 纠删编码
- regions
- 存储池

用户必须具有 * 其他网格配置 * 和 * 网格拓扑页面配置 * 权限才能管理存储级别。

维护

用户必须具有维护权限才能使用以下选项：

- * 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
  - 对象存在检查
  - 恢复
- * 维护 * > * 系统 * ：
  - 恢复包
  - 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以下页面：

- * 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 * > * 安全性 * ：
  - 证书
- * 配置 * > * 监控 * ：
  - 审核和系统日志服务器

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。

指标查询

此权限提供对以下内容的访问权限：

- **support**>*Tools*>*Metrics *页面
- 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信息板卡

对象元数据查找

通过此权限，您可以访问 * ILM * > * 对象元数据查找 * 页面。

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。

- * ILM ：
  - 存储等级
- * 配置 * > * 系统 * ：
  - 存储选项
- * 支持 * > * 警报（传统） * ：
  - 自定义事件
  - 全局警报
  - 传统电子邮件设置
- 支持>*其他*：
  - 链路成本

存储设备管理员

此权限提供：

- 通过网格管理器访问存储设备上的E系列SANtricity System Manager。
- 能够在管理驱动器选项卡上对支持这些操作的设备执行故障排除和维护任务。

租户帐户

此权限可用于：

- 访问租户页面、在此可以创建、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Grid Manager信息板卡

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网格管理器功能。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "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，并将每个用户分配给一个或多个本地组。组的权限控制用户可以访问的网格管理器和网格管理 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。

如果启用了单点登录(SSO)、则本地用户无法登录到StorageGRID。

访问向导

步骤

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

输入用户凭据

步骤

1. 输入用户的全名，唯一用户名和密码。

2. 或者，如果此用户不应访问网格管理器或网格管理 API ，请选择 * 是 * 。
3. 选择 * 继续 * 。

分配给组

步骤

1. （可选）将用户分配给一个或多个组以确定用户的权限。

   如果尚未创建组，则可以保存用户而不选择组。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 "管理管理组" 了解详细信息。

2. 选择 * 创建用户 * 并选择 * 完成 * 。

查看和编辑本地用户

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用户的全名，密码或组成员资格。您还可以暂时阻止用户访问网格管理器和网格管理 API 。

您只能编辑本地用户。使用外部身份源管理联合用户。

- 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。
- 要查看特定用户的所有详细信息，编辑本地用户或更改本地用户的密码，请使用 * 操作 * 菜单或详细信息页面。

  用户下次注销后重新登录到网格管理器时，系统将应用任何编辑。

  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。

任务	操作菜单	详细信息页面
查看用户详细信息	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。	在表中选择用户名。
编辑全名（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 编辑全名 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	a. 选择用户的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 * 保存更改 * 。

任务	操作菜单	详细信息页面
拒绝或允许 StorageGRID 访问	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择访问选项卡。 d. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 e. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择访问选项卡。 c. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 d. 选择 * 保存更改 * 。
更改密码（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择密码选项卡。 d. 输入新密码。 e. 选择 * 更改密码 * 。	a. 选择用户的名称以显示详细信息。 b. 选择密码选项卡。 c. 输入新密码。 d. 选择 * 更改密码 * 。
更改组（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择组选项卡。 d. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 e. 选择 * 编辑组 * 以选择不同的组。 f. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择组选项卡。 c. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 d. 选择 * 编辑组 * 以选择不同的组。 e. 选择 * 保存更改 * 。

复制用户

您可以复制现有用户以创建具有相同权限的新用户。

步骤

1. 选中用户对应的复选框。
2. 选择 * 操作 * > * 复制用户 * 。
3. 完成复制用户向导。

删除用户

您可以删除本地用户，以便从系统中永久删除该用户。

您不能删除root用户。

步骤

1. 在用户页面中、选中要删除的每个用户对应的复选框。
2. 选择 * 操作 * > * 删除用户 * 。
3. 选择 * 删除用户 * 。

使用单点登录（ SSO ）

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 。本地用户无法登录到StorageGRID。

单点登录的工作原理

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 后 StorageGRID 登录和注销过程会受到什么影响。

启用 **SSO** 后登录

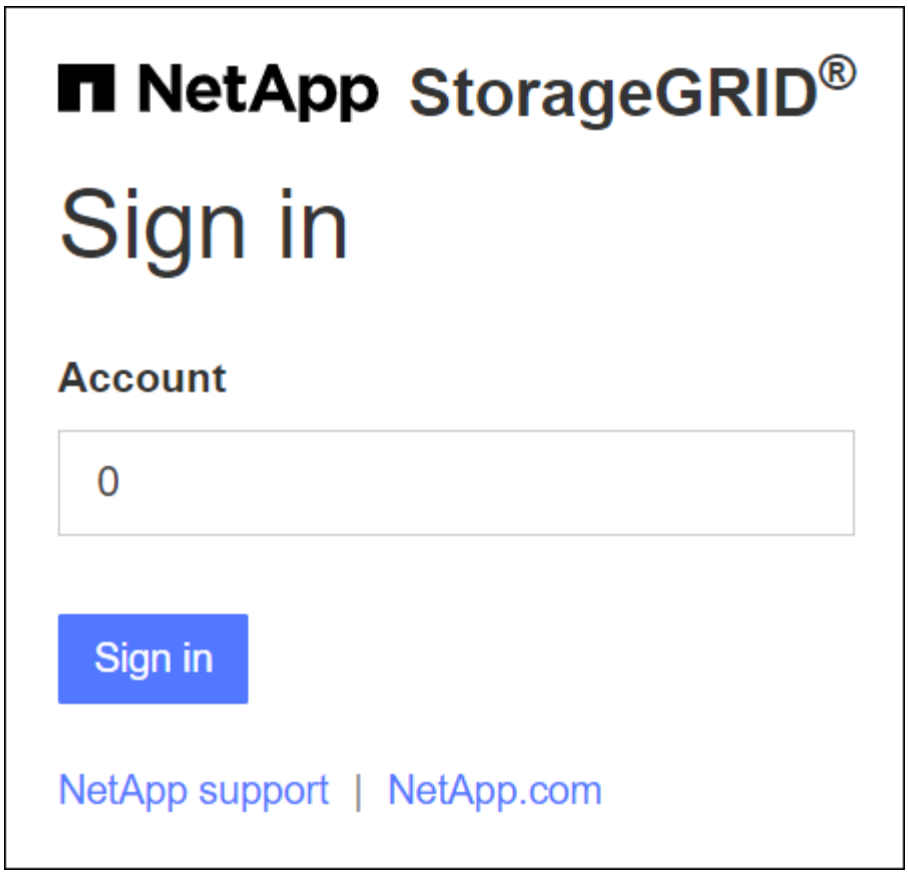
启用 SSO 并登录到 StorageGRID 后，系统会将您重定向到组织的 SSO 页面以验证您的凭据。

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 ：

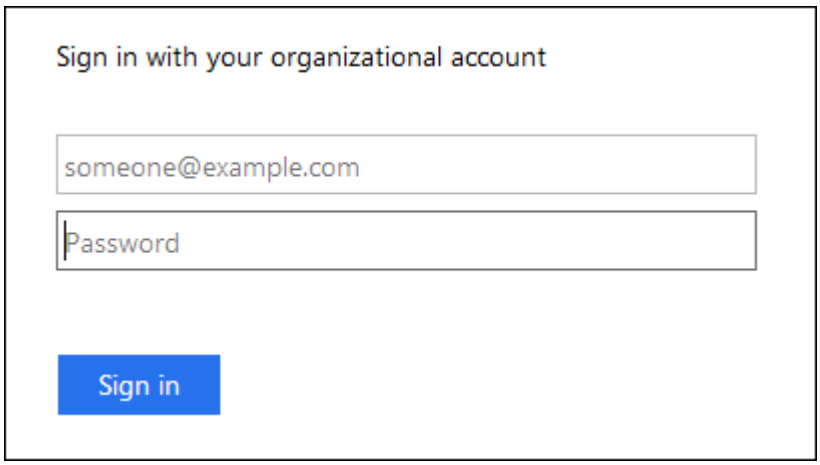


◦ 如果您之前访问过网格管理器或租户管理器，系统将提示您选择最近的帐户或输入帐户 ID：

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 ，或者选择 * 网格管理器 * （如果它显示在近期帐户列表中）。
   - 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. 选择 * 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 StorageGRID 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。

      如果此服务帐户不可访问，则只要您是具有 StorageGRID 访问权限的联合组的现有用户，您仍可登录。

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. 在用户界面右上角找到*Sign Out (注销)*链接。
2. 选择*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 • 注意： * 如果您使用 Azure 进行 SSO ，则从所有管理节点中注销可能需要几分钟的时间。
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。

单点登录的要求和注意事项

在为StorageGRID 系统启用单点登录(Single Sign On、SSO)之前、请查看相关要求和注意事项。

身份提供程序要求

StorageGRID 支持以下 SSO 身份提供程序（ IdP ）：

- Active Directory 联合身份验证服务（ AD FS ）
- Azure Active Directory （ Azure AD ）
- 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 服务类型控制您可以实施的 SSO 类型。

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

AD FS 要求

您可以使用以下任意版本的 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（ Transport Layer Security ， TLS ） 1.2 或 1.3
- Microsoft .NET Framework 3.5.1 或更高版本

Azure注意事项

如果您使用Azure作为SSO类型、并且用户的用户主体名称未使用sAMAccountName作为前缀、则在StorageGRID 与LDAP服务器断开连接时可能会出现登录问题。要允许用户登录、您必须还原与LDAP服务器的连接。

服务器证书要求

默认情况下， StorageGRID 会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。在为 StorageGRID 配置依赖方信任（ AD FS ），企业应用程序（ Azure ）或服务提供商连接（ PingFederate ）时，您可以使用服务器证书作为 StorageGRID 请求的签名证书。

如果您尚未执行此操作 "已为管理接口配置自定义证书"，您现在应执行此操作。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，企业应用程序或 SP 连接中使用该证书。

建议不要在依赖方信任，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依赖方信任，企业应用程序或 SP 连接。

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`。

端口要求

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 ）。请参见 "在外部防火墙处控制访问"。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您已配置身份联合。

步骤

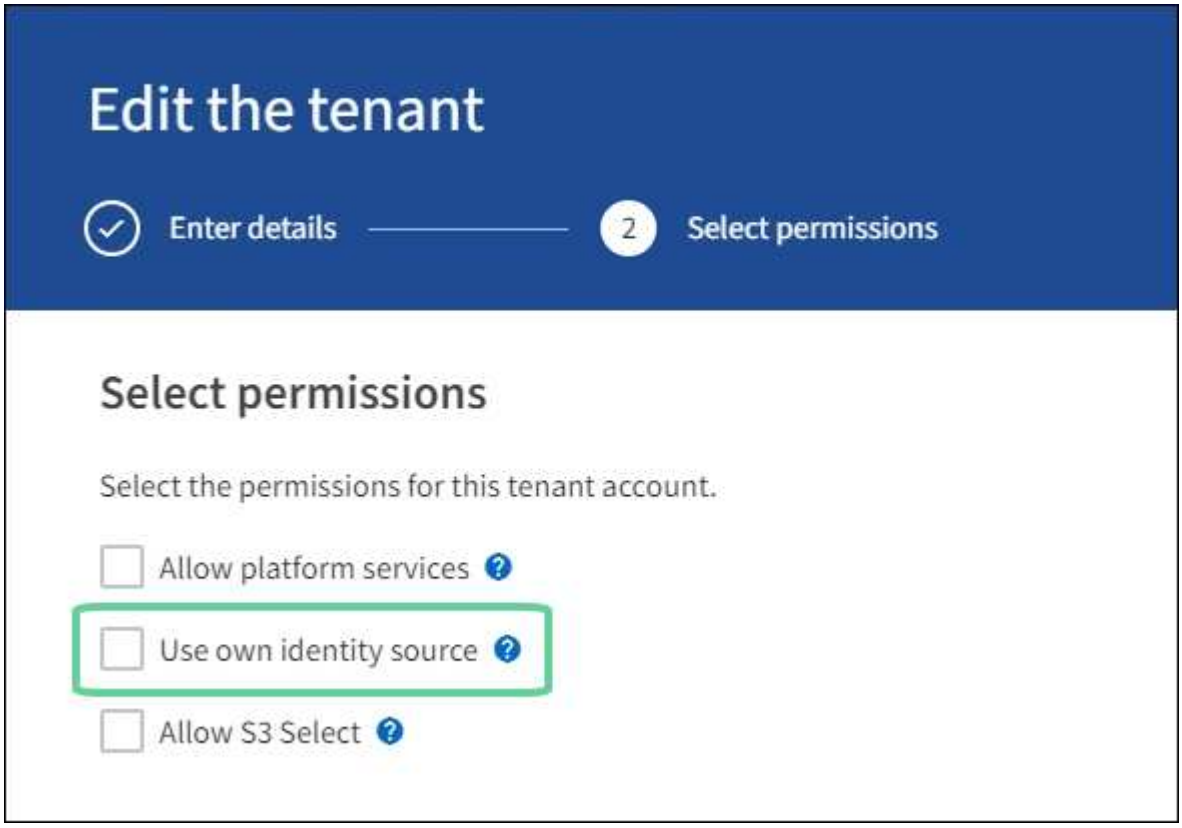
1. 如果存在现有租户帐户，请确认所有租户均未使用其自己的身份源。

> 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、请确认不再需要此租户帐户可能正在使用的任何联盟组、清除此复选框、然后选择*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 root 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，然后选择 * 操作 * > * 编辑 * 。
   c. 在输入详细信息选项卡上，选择 * 继续 * 。
   d. 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并选择*保存*。



此时将显示租户页面。

a. 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。
b. 在租户管理器中，选择 * 访问管理 * > * 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 root 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

- "单点登录的要求和注意事项"
- "管理管理组"
- "使用租户帐户"

使用沙盒模式

在为所有 StorageGRID 用户启用单点登录（ SSO ）之前，您可以使用沙盒模式配置和测试单点登录（ SSO ）。启用 SSO 后，您可以在需要更改或重新测试配置时返回到沙盒模式。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "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 * ，您根据计划使用的 SSO 身份提供程序选择了 Active Directory 或 Azure 。

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

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 SSO 身份提供程序发送身份验证请求。然后， SSO 身份提供程序会向 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 的响应包括用户的通用唯一标识符（ UUID ）。
- Azure 的响应包括用户主体名称（ UPN ）。

要允许 StorageGRID （服务提供商）和 SSO 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 SSO 身份提供程序的软件为每个管理节点创建依赖方信任（ AD FS ），企业应用程序（ Azure ）或服务提供商（ PingFederate ）。最后，您必须返回到 StorageGRID 以启用 SSO 。

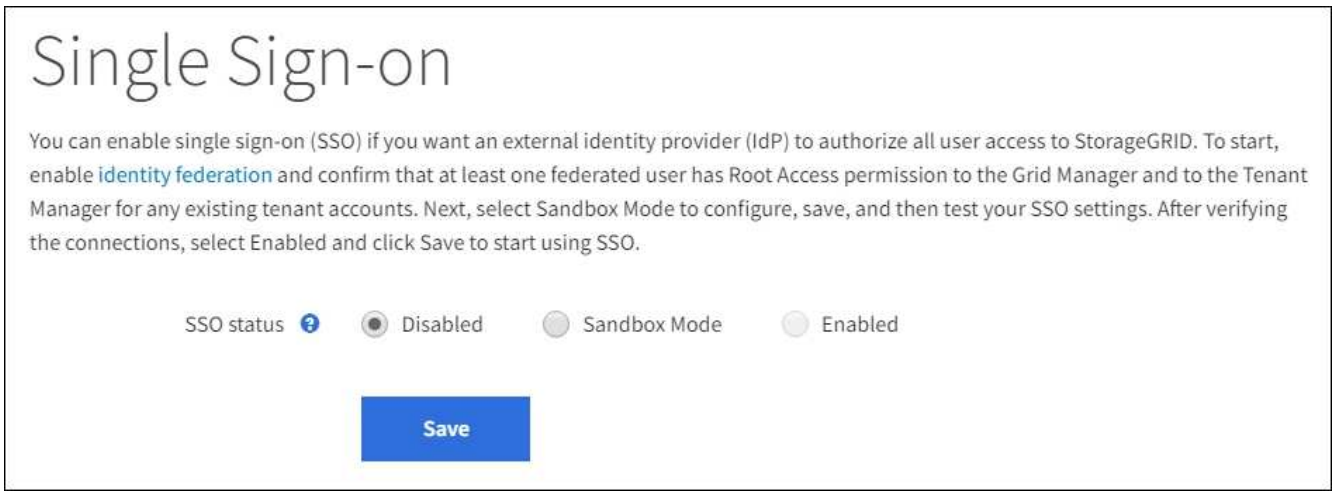
使用沙盒模式，可以轻松执行此背面配置，并在启用 SSO 之前测试所有设置。使用沙盒模式时、用户无法使用SSO登录。

访问沙盒模式

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、请确认已将身份提供程序配置为联合身份源。请参见 "单点登录的要求和注意事项"。

2. 选择 * 沙盒模式 * 。

   此时将显示 "Identity Provider" 部分。

输入身份提供程序详细信息

步骤

1. 从下拉列表中选择 * SSO 类型 * 。
2. 根据您选择的 SSO 类型填写身份提供程序部分中的字段。

Active Directory

1. 输入身份提供程序的 * 联合服务名称 * ，与 Active Directory 联合身份验证服务（ AD FS ）中显示的名称完全相同。

   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。

2. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 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，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。
   - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。

     如果更改CA证书、请立即执行 "在管理节点上重新启动mgmt-api服务" 并测试是否已成功通过SSO访问网格管理器。

3. 在依赖方部分中，指定 StorageGRID 的 * 依赖方标识符 * 。此值控制 AD FS 中每个依赖方信任所使用的名称。
   - 例如、如果您的网格只有一个管理节点、并且您不希望将来添加更多管理节点、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]`。此时将生成一个表，其中根据节点的主机名显示系统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。

4. 选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

Azure 酒店

1. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 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，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

- * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。

> 如果更改CA证书、请立即执行 "在管理节点上重新启动mgmt-api服务" 并测试是否已成功通过SSO访问网格管理器。

2. 在企业应用程序部分中，为 StorageGRID 指定 * 企业应用程序名称 * 。此值控制 Azure AD 中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、并且您不希望将来添加更多管理节点、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]`。此时将生成一个表，其中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级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

3. 按照中的步骤进行操作 "在 Azure AD 中创建企业级应用程序" 为表中列出的每个管理节点创建企业级应用程序。
4. 从 Azure AD 中，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 中相应的 * 联合元数据 URL* 字段中。
5. 复制并粘贴所有管理节点的联合元数据 URL 后，选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

PingFederate

1. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。

   - * 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，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

   - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。

> 如果更改CA证书、请立即执行 "在管理节点上重新启动mgmt-api服务" 并测试是否已成功通过SSO访问网格管理器。

2. 在服务提供商（ SP ）部分中，为 StorageGRID 指定 * SP 连接 ID* 。此值控制 PingFederate 中每个 SP 连接使用的名称。

   - 例如、如果您的网格只有一个管理节点、并且您不希望将来添加更多管理节点、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]`。此时将生成一个表，其中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一个 SP 连接。为每个管理节点建立 SP 连接可确保用户可以安全地登录和注销任何管理节点。

3. 在 * 联合元数据 URL* 字段中指定每个管理节点的联合元数据 URL 。

   请使用以下格式：

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

4. 选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

配置依赖方信任，企业应用程序或 **SP** 连接

保存配置后，将显示沙盒模式确认通知。此通知用于确认沙盒模式现已启用，并提供了概述说明。

只要需要， StorageGRID 就可以保持沙盒模式。但是，如果在 Single Sign-On 页面上选择了 * 沙盒模式 * ，则所有 StorageGRID 用户都将禁用 SSO 。只有本地用户才能登录。

按照以下步骤配置依赖方信任（ Active Directory ），完整的企业应用程序（ Azure ）或配置 SP 连接（ PingFederate ）。

Active Directory

步骤

1. 转至 Active Directory 联合身份验证服务（ AD FS ）。
2. 使用 StorageGRID 单点登录页面上的表中所示的每个依赖方标识符为 StorageGRID 创建一个或多个依赖方信任。

   您必须为表中所示的每个管理节点创建一个信任。

   有关说明，请转至 "在 AD FS 中创建依赖方信任"。

Azure 酒店

步骤

1. 从当前登录到的管理节点的单点登录页面中，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. 按照中的步骤进行操作 "在 Azure AD 中创建企业级应用程序" 将每个管理节点的 SAML 元数据文件上传到其对应的 Azure 企业应用程序中。

PingFederate

步骤

1. 从当前登录到的管理节点的单点登录页面中，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 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 （如 StorageGRID 单点登录页面上的表所示）以及为该管理节点下载的 SAML 元数据。

   您必须为表中所示的每个管理节点创建一个 SP 连接。

测试 **SSO** 连接

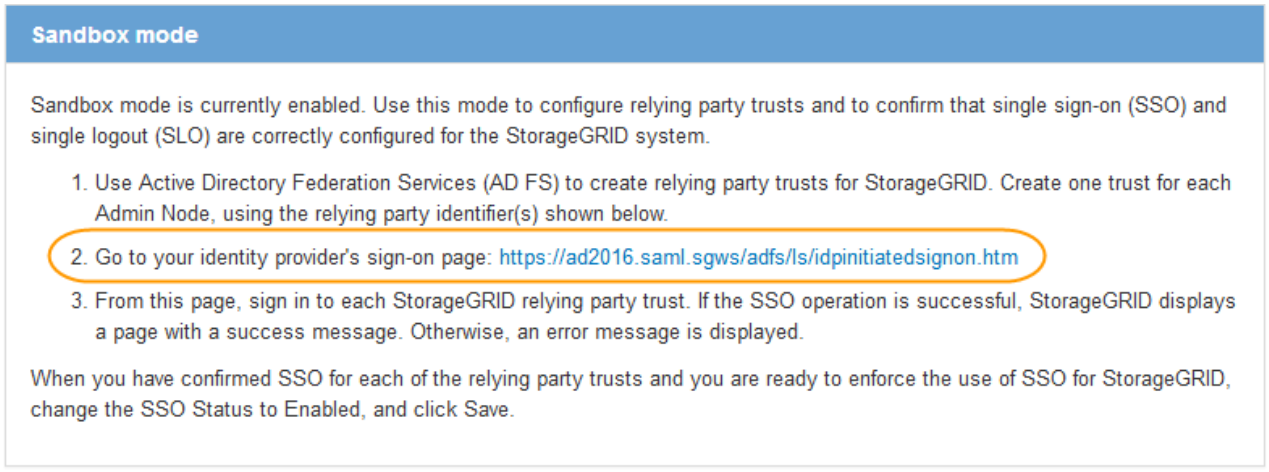
在对整个 StorageGRID 系统强制使用单点登录之前，您应确认已为每个管理节点正确配置单点登录和单点注销。

Active Directory

步骤

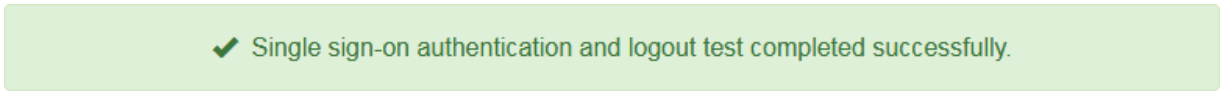
1. 在 StorageGRID 单点登录页面中，找到沙盒模式消息中的链接。

   此 URL 是从您在 * 联合服务名称 * 字段中输入的值派生的。



2. 选择此链接，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。
3. 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，然后选择 * 登录 * 。

4. 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。
5. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

Azure 酒店

步骤

1. 转到 Azure 门户中的单点登录页面。
2. 选择 * 测试此应用程序 * 。
3. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

     ✔ Single sign-on authentication and logout test completed successfully.

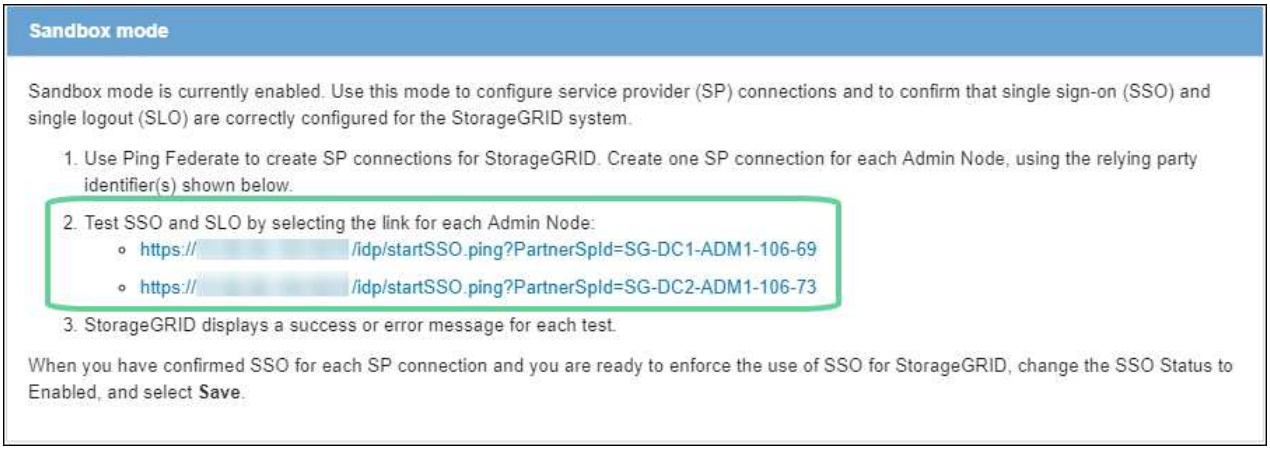
   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
4. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

PingFederate

步骤

1. 从 StorageGRID 单点登录页面中，选择沙盒模式消息中的第一个链接。

   一次选择并测试一个链路。



2. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

     ✔ Single sign-on authentication and logout test completed successfully.

   - 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。
3. 选择下一个链接以验证网格中每个管理节点的 SSO 连接。

   如果您看到页面已过期消息，请在浏览器中选择 * 返回 * 按钮，然后重新提交您的凭据。

启用单点登录

确认可以使用 SSO 登录到每个管理节点后，您可以为整个 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. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
2. 将 SSO 状态更改为 * 已启用 * 。
3. 选择 * 保存 * 。
4. 查看警告消息，然后选择 * 确定 * 。

   现在，已启用单点登录。

如果您使用的是 Azure 门户，并且从用于访问 Azure 的同一计算机访问 StorageGRID ，请确保 Azure 门户用户也是授权的 StorageGRID 用户（已导入到 StorageGRID 的联合组中的用户） 或者，在尝试登录到 StorageGRID 之前，请先从 Azure 门户中注销。

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。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择了 * AD FS* 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 "使用沙盒模式"。
- 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 单点登录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。
- 如果您要手动创建依赖方信任，则可以获得为 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。

关于此任务

以下说明适用于 Windows Server 2016 AD FS 。如果您使用的是其他版本的 AD FS ，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。

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。

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"

   - 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. 选择 * 应用 * ，然后选择 * 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. 选择 * 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 * ，然后选择 * 下一步 * 。
   e. 在配置规则页面上，输入此规则的显示名称。

      例如，**ObjectGUID**到名称**ID***或***UPN**到名称**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*objectGUID*或选择*User-Principal-Name*。
   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. 选择 * 完成 * ，然后选择 * 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、请确认联盟元数据地址是否正确、或者手动输入值。

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 并测试所有相关方信任，以确认其配置正确。请参见 "使用沙盒模式" 有关说明，请参见。

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 管理 * 。
2. 在操作下，选择 * 添加依赖方信任 * 。
3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 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. 选择 * 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 * ，然后选择 * 下一步 * 。
   d. 在配置规则页面上，输入此规则的显示名称。

      例如，**ObjectGUID**到名称**ID***或***UPN**到名称**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*objectGUID*或选择*User-Principal-Name*。
   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. 选择 * 完成 * ，然后选择 * 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、请确认联盟元数据地址是否正确、或者手动输入值。

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 并测试所有相关方信任，以确认其配置正确。请参见 "使用沙盒模式" 有关说明，请参见。

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。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * ，然后选择 * AD FS 管理 * 。
2. 在操作下，选择 * 添加依赖方信任 * 。
3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 开始 * 。
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 Claim Rule 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 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。

   b. 在配置规则页面上，输入此规则的显示名称。

例如，**ObjectGUID**到名称**ID***或***UPN**到名称**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*objectGUID*或选择*User-Principal-Name*。

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. 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 * 端点 * 选项卡上，为单点注销（ SLO ）配置端点：

a. 选择 * 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. 选择 * 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. 选择 * 应用 * ，然后选择 * 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 并测试所有相关方信任，以确认其配置正确。请参见 "使用沙盒模式" 有关说明，请参见。

在 **Azure AD** 中创建企业级应用程序

您可以使用 Azure AD 为系统中的每个管理节点创建企业级应用程序。

开始之前

- 您已开始为 StorageGRID 配置单点登录，并选择了 * Azure * 作为 SSO 类型。

- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 "使用沙盒模式"。
- 系统中每个管理节点都有 * 企业级应用程序名称 * 。您可以从 StorageGRID 单点登录页面上的管理节点详细信息表复制这些值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个企业级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

- 您有在 Azure Active Directory 中创建企业级应用程序的经验。
- 您有一个 Azure 帐户且订阅有效。
- 您在 Azure 帐户中具有以下角色之一：全局管理员，云应用程序管理员，应用程序管理员或服务主体的所有者。

访问 **Azure AD**

步骤

1. 登录到 "Azure 门户"。
2. 导航到 "Azure Active Directory"。
3. 选择 … "企业级应用程序"。

创建企业级应用程序并保存 **StorageGRID SSO** 配置

要在StorageGRID 中保存Azure的SSO配置、您必须使用Azure为每个管理节点创建一个企业应用程序。您将从 Azure 复制联合元数据 URL ，并将其粘贴到 StorageGRID Single Sign-On 页面上对应的 * 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 Azure Enterprise 应用程序窗格中，选择 * 新建应用程序 * 。
    b. 选择 * 创建您自己的应用程序 * 。
    c. 对于此名称，请输入您从 StorageGRID Single Sign-On 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 * 集成在库（非库）中找不到的任何其他应用程序 * 单选按钮。
    e. 选择 * 创建 * 。
    f. 选择 * 。 2.设置单点登录 * 框，或者选择左侧边距中的 * 单点登录 * 链接。
    g. 选择 * SAML * 框。
    h. 复制 * 应用程序联合元数据 URL* ，该 URL 可在 * 步骤 3 SAML 签名证书 * 下找到。
    i. 转到 StorageGRID 单点登录页面，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 配置进行所有其他所需更改后，请在 StorageGRID Single Sign-On 页面上选择 * 保存 * 。

下载每个管理节点的 **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上述步骤。
   a. 从管理节点登录到 StorageGRID 。
   b. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   c. 选择按钮以下载此管理节点的 SAML 元数据。
   d. 保存要上传到 Azure AD 的文件。

将 **SAML** 元数据上传到每个企业级应用程序

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

步骤

1. 返回到 Azure 门户。
2. 对每个企业级应用程序重复以下步骤：

   您可能需要刷新 " 企业应用程序 " 页面才能查看先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 * （除非您要单独配置分配）。
   c. 转到单点登录页面。
   d. 完成 SAML 配置。
   e. 选择 * 上传元数据文件 * 按钮，然后选择为相应管理节点下载的 SAML 元数据文件。
   f. 加载文件后，选择 * 保存 * ，然后选择 * X * 以关闭窗格。此时将返回到使用 SAML 设置单点登录页面。
3. 按照中的步骤进行操作 "使用沙盒模式" 测试每个应用程序。

在 **PingFederate** 中创建服务提供商（ **SP** ）连接

您可以使用 PingFederate 为系统中的每个管理节点创建服务提供商（ SP ）连接。要加快此过程，您需要从 StorageGRID 导入 SAML 元数据。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择了 * Ping 联邦 * 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 "使用沙盒模式"。
- 您拥有系统中每个管理节点的 * SP 连接 ID* 。您可以在 StorageGRID 单点登录页面上的管理节点详细信息表中找到这些值。
- 您已为系统中的每个管理节点下载 * SAML 元数据 * 。
- 您在 PingFederate 服务器中创建 SP 连接的经验。

- 您拥有 "《管理员参考指南》" PingFederate 服务器。PingFederate 文档提供了详细的分步说明和说明。
- 您拥有 "管理员权限" PingFederate 服务器。

关于此任务

以下说明总结了如何将 PingFederate 服务器 10.3 版配置为 StorageGRID 的 SSO 提供程序。如果您使用的是其他版本的 PingFederate ，则可能需要调整这些说明。有关您的版本的详细说明，请参见 PingFederate 服务器文档。

完成 **PingFederate** 中的前提条件

在创建要用于 StorageGRID 的 SP 连接之前，必须先在 PingFederate 中完成前提条件任务。配置 SP 连接时，您将使用这些前提条件中的信息。

创建数据存储库**[Data -store]]**

如果尚未创建数据存储库，请将 PingFederate 连接到 AD FS LDAP 服务器。使用您在使用时使用的值 "配置身份联合" 在 StorageGRID 中。

- * 类型 * ： 目录（ LDAP ）
- * LDAP 类型 * ： Active Directory
- * 二进制属性名称 * ： 在 "LDAP 二进制属性 " 选项卡上输入 * 对象 GUID* ，具体如图所示。

创建密码凭据验证器**[password-validator]]**

如果尚未创建密码凭据验证程序，请创建一个。

- * 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。
- * 搜索基础 * ： 输入 LDAP 中的信息（例如， DC=SAML ， DC=sgws ）。
- * 搜索筛选器 * ： sAMAccountName=$ ｛username ｝
- * 范围 * ： 子树

创建**IdP**适配器实例**[adapter-instance]]**

如果尚未创建 IdP 适配器实例，请创建此实例。

步骤

1. 转至 * 身份验证 * > * 集成 * > * IdP 适配器 * 。
2. 选择 * 创建新实例 * 。
3. 在类型选项卡上，选择 * HTML 表单 IdP 适配器 * 。
4. 在 IdP 适配器选项卡上，选择 * 向 " 凭据验证器 "* 添加新行。
5. 选择 密码凭据验证程序 您已创建。
6. 在适配器属性选项卡上，为 * 伪名称 * 选择 * 用户名 * 属性。
7. 选择 * 保存 * 。

创建或导入签名证书

如果尚未创建，请创建或导入签名证书。

步骤

1. 转至 * 安全性 * > * 签名和解密密钥和证书 * 。
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，您可以导入从 StorageGRID 为管理节点下载的 SAML 元数据。元数据文件包含您需要的许多特定值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个 SP 连接，以便用户可以安全地登录和注销任何节点。按照以下说明创建第一个 SP 连接。然后，转到 创建其他 SP 连接 创建所需的任何其他连接。

选择 **SP** 连接类型

步骤

1. 转至 * 应用程序 * > * 集成 * > * SP 连接 * 。
2. 选择 * 创建连接 * 。
3. 选择 * 不对此连接使用模板 * 。
4. 选择 * 浏览器 SSO 配置文件 * 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. 选择从管理节点的 StorageGRID 单点登录页面下载的 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 * 下一步 * 。

配置 **IdP** 浏览器 **SSO**

步骤

1. 从浏览器 SSO 选项卡中，选择 * 配置浏览器 SSO* 。
2. 在 SAML 配置文件选项卡上，选择 * SP 启动的 SSO* ， * SP 初始 SLO* ， * IdP-Initiated SSO* 和 * IdP-Initiated SLO* 选项。
3. 选择 * 下一步 * 。
4. 在 Assertion Lifetime 选项卡上，不进行任何更改。
5. 在断言创建选项卡上，选择 * 配置断言创建 * 。

a. 在身份映射选项卡上，选择 * 标准 * 。

b. 在属性合同选项卡上，使用 * SAML 主题 * 作为属性合同以及导入的未指定名称格式。

6. 要延长合同，请选择*Delete*以删除 `urn:oid`，未使用。

映射适配器实例

步骤

1. 在身份验证源映射选项卡上，选择 * 映射新适配器实例 * 。
2. 在适配器实例选项卡上，选择 适配器实例 您已创建。
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，提供问题描述 并选择 数据存储 您已添加。
6. 在 LDAP 目录搜索选项卡上：
   - 输入 * 基本 DN* ，该 DN 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，请选择 * 子树 * 。
   - 对于根对象类，搜索并添加以下属性之一：**objectGUUD***或***userPrincipalName**。
7. 在 LDAP 二进制属性编码类型选项卡上，为 * 对象 GUID* 属性选择 * Base64* 。
8. 在 LDAP 筛选器选项卡上，输入 * 。 sAMAccountName=$ ｛username｝ * 。
9. 在属性合同履行选项卡上，从来源下拉列表中选择*LDAP (属性)，然后从值下拉列表中选择***objectGUID*** 或***userPrincipalName**。
10. 查看并保存属性源。
11. 在故障保存属性源选项卡上，选择 * 中止 SSO 事务 * 。
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* > * 浏览器 SSO* > * 协议设置 * 选项卡上，选择 * 配置协议设置 * 。
2. 在断言使用方服务URL选项卡上、接受从StorageGRID SAML元数据导入的默认值(* post*用于绑定和 `/api/saml-response` 表示端点URL)。
3. 在SLO服务URL选项卡上、接受从StorageGRID SAML元数据导入的默认值(*重定向*用于绑定和) `/api/saml-logout` 端点URL。
4. 在允许的SAML绑定选项卡上、清除*项目*和* SOAP *。仅需要 * 发布 * 和 * 重定向 * 。
5. 在“签名策略”选项卡上，保持选中“要求对authn请求进行签名”和“始终签名断言”复选框。
6. 在加密策略选项卡上，选择 * 无 * 。
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. 从 SP 连接选项卡中，选择 * 凭据 * 。
2. 从凭据选项卡中，选择 * 配置凭据 * 。
3. 选择 正在签名证书 您已创建或导入。
4. 选择 * 下一步 * 转到 * 管理签名验证设置 * 。
   a. 在信任模式选项卡上，选择 * 已取消锁定 * 。
   b. 在签名验证证书选项卡上，查看从 StorageGRID SAML 元数据导入的签名证书信息。
5. 查看摘要屏幕并选择 * 保存 * 以保存 SP 连接。

创建其他 **SP** 连接

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

> 不同管理节点的 SP 连接使用相同的设置，但合作伙伴的实体 ID ，基本 URL ，连接 ID ，连接名称，签名验证除外。 和 SLO 响应 URL 。

步骤

1. 选择 * 操作 * > * 复制 * 为每个附加管理节点创建初始 SP 连接的副本。
2. 输入副本的连接 ID 和连接名称，然后选择 * 保存 * 。
3. 选择与管理节点对应的元数据文件：
   a. 选择 * 操作 * > * 使用元数据更新 * 。
   b. 选择 * 选择文件 * 并上传元数据。
   c. 选择 * 下一步 * 。
   d. 选择 * 保存 * 。
4. 解决由于属性未使用而导致的错误：
   a. 选择新连接。
   b. 选择 * 配置浏览器 SSO > 配置断言创建 > 属性合同 * 。
   c. 删除 * urn ： oid* 的条目。
   d. 选择 * 保存 * 。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "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 Single Sign-On 页面。

2. 选择 * 已禁用 * 选项。
3. 选择 * 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. 选择 * 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 。

开始之前

- 您已拥有 "特定访问权限"。
- 您拥有 `Passwords.txt` 文件
- 您知道本地 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。网格管理器中单点登录页面上的*Enable SSO*复选框保持选中状态，所有现有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. 选择 * 保存 * 。

      从 Single Sign-On 页面选择 * 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. 选择*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。

版权信息

商标信息