使用单点登录（SSO）

StorageGRID software

NetApp
February 12, 2026

目录

使用单点登录（ SSO ）

SSO 的工作原理

启用单点登录 (SSO) 后，只有使用贵组织实施的 SSO 登录流程授权用户的凭据后，用户才可以访问网格管理器、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 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。

   - 如果这是您第一次通过此浏览器访问该 URL，系统会提示您输入帐户 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。

   > 如果输入租户帐户的完整StorageGRID (即完全限定域名或IP地址，后跟)，则不会显示“URL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，您可以在该页面中使用您的 SSO 凭据登录进行登录。

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。

   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。

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 Entra ID 进行 SSO，则可能需要几分钟才能退出所有管理节点。
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 。

SSO 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 ）
- 微软Entra ID

- 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 • 进入 ID • PingFederate
进入 ID	进入 ID

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

Entra ID 的注意事项

如果您使用 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 服务器失去连接时，可能会出现登录问题。要允许用户登录，您必须恢复与 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。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，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"已为管理接口配置自定义证书"执行此操作，则应立即执行此操作。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并转到目录来访问此节点的服务器证书 `/var/local/mgmt-api`。自定义服务器证书名为 `custom-server.crt`。此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 ）。请参阅。 "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

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "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. 从网格管理器中，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. 从网格管理器中，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。

   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. 从租户管理器中，选择*访问管理*>*组*。

g. 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。

h. 注销。

i. 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"

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)，然后为所有StorageGRID用户启用它。启用 SSO 后，您可以在需要时返回沙盒模式来更改或重新测试配置。

开始之前

- 您已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，您可以根据计划使用的 SSO 身份提供商选择 Active Directory 或 Entra ID。

已配置 **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 • 进入 ID • PingFederate
进入 ID	进入 ID

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 ）。
- Entra ID 的响应包括用户主体名称 (UPN)。

为了允许StorageGRID （服务提供商）和 SSO 身份提供商就用户身份验证请求进行安全通信，您需要完成以下任务：

1. 在StorageGRID中配置设置。

2. 使用 SSO 身份提供商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 (Entra ID) 或服务提供商 (PingFederate)。
3. 返回StorageGRID以启用 SSO。

沙盒模式可以轻松执行这种来回配置，并在启用 SSO 之前测试所有设置。当您使用沙盒模式时，用户无法使用 SSO 登录。

访问向导

步骤

1. 选择*配置* > 访问控制 > 单点登录。出现“单点登录”页面。

> 如果配置 SSO 设置按钮被禁用，请确认您已将身份提供者配置为联合身份源。请参阅"单点登录的要求和注意事项" 。

2. 选择*配置 SSO 设置*。出现提供身份提供者详细信息页面。

提供身份提供者详细信息

步骤

1. 从下拉列表中选择 * SSO 类型 * 。
2. 如果您选择 Active Directory 作为 SSO 类型，请输入身份提供者的 联合身份验证服务名称，与 Active Directory 联合身份验证服务 (AD FS) 中显示的完全一致。

> 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。

3. 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。

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

4. 选择*继续*。出现“提供依赖方标识符”页面。

提供依赖方标识符

1. 根据您选择的 SSO 类型填写“提供依赖方标识符”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 中为每个信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`。
   - 如果您的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]` 。包含此字符串将生成一个表，该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。

b. 选择*保存并进入沙盒模式*。

进入 **ID**

a. 在企业应用程序部分，指定StorageGRID的 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，并且您不希望将来添加更多管理节点，请输入 `SG`或 `StorageGRID`。
   - 如果您的网格包含多个管理节点，请包含字符串 `[HOSTNAME]`在标识符中。例如， `SG-[HOSTNAME]` 。包含此字符串将生成一个表，该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。

b. 按照以下步骤操作"在 Entra ID 中创建企业应用程序"为表中列出的每个管理节点创建一个企业应用程序。

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中相应的 **Federation metadata URL** 字段中。

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

PingFederate

a. 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`。
   - 如果您的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]` 。包含此字符串将生成一个表，该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。

b. 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>
```

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可以登录。

Active Directory

步骤

1. 转至 Active Directory 联合身份验证服务（ AD FS ）。
2. 使用“配置 SSO”页面上的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。

   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"。

进入 **ID**

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. 按照以下步骤操作"在 Entra ID 中创建企业应用程序"将每个管理节点的 SAML 元数据文件上传到其对应的 Entra ID 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（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。

   您必须为表中所示的每个管理节点创建一个 SP 连接。

测试配置

在强制整个StorageGRID系统使用单点登录之前，请确认每个管理节点的单点登录和单点注销均已正确配置。

Active Directory

步骤

1. 在配置 SSO 页面上，找到向导的测试配置步骤上的链接。

   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。

进入 **ID**

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

   单点登录现已启用。出现“单点登录”页面，其中现在包含您刚刚配置的 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“禁用 **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 门户用户也是授权的StorageGRID用户（已导入StorageGRID 的联合组中的用户），或者在尝试登录StorageGRID之前注销 Azure 门户。

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。
- 你有"进入沙盒模式"在网格管理器中。
- 您知道系统中每个管理节点的完全限定域名（或 IP 地址）和信赖方标识符。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"
   ```

   - 对于 *Admin_Node_Identifier*，输入管理节点的“依赖方标识符”，与它在“单一登录”页面上显示的完全相同。例如， `SG-DC1-ADM1`。
   - 对于 *Admin_Node_FQDN*，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StorageGRID并"测试所有依赖方信任"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 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`

   对于 *Admin_Node_FQDN*，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StorageGRID并"测试所有依赖方信任"确认它们配置正确。

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。

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`

      对于 *Admin_Node_FQDN*，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

      对于 *Admin_Node_Identifier*，输入管理节点的“依赖方标识符”，与它在“单一登录”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
```

对于 *Admin_Node_FQDN*，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、转到管理节点的目录、 `/var/local/mgmt-api`然后添加`custom-server.crt`证书文件。

(`server.crt`不建议使用管理节点的默认证书)。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StorageGRID并"测试所有依赖方信任"确认它们配置正确。

在 Entra ID 中创建企业应用程序

您使用 Entra ID 为系统中的每个管理节点创建一个企业应用程序。

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。

- 你有"进入沙盒模式"在网格管理器中。
- 您的系统中的每个管理节点都有*企业应用程序名称*。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 Entra ID 中创建企业应用程序的经验。
- 您有一个具有有效订阅的 Entra ID 帐户。
- 您在 Entra ID 帐户中拥有以下角色之一：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 **Entra ID**

步骤

1. 登录到 "Azure 门户"。
2. 导航至 "进入 ID"。
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 Entra ID 的 SSO 配置，您必须使用 Entra ID 为每个管理节点创建一个企业应用程序。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 新应用程序。
   b. 选择 * 创建您自己的应用程序 * 。
   c. 对于名称，请输入从配置 SSO 页面上的管理节点详细信息表复制的*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. 转到配置 SSO 页面，并将 URL 粘贴到与您使用的 企业应用程序名称 相对应的 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的更改后，在配置 SSO 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. 保存文件，然后将其上传到 Entra ID。

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 Entra ID 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. "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。
- 你有"进入沙盒模式"在网格管理器中。
- 您系统中每个管理节点都有* 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。
- 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。
- 您有https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["《管理员参考指南》"^]用于PingFedate服务器的。PingFederate 文档提供了详细的分步

说明和说明。

- 你有"管理员权限"用于 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StorageGRID中使用的值"配置身份联合"。

- * 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你创造的。
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 * 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*以删除未使用的 `urn:oid`。

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 * 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(绑定和端点URL的*post* `/api/saml-response`)。
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*用于绑定和端点URL) `/api/saml-logout`。
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创建或导入的。
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 SSO

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

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "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*禁用 SSO*。
3. 选择 * 是 * 。

   此时将显示一条警告消息，指示本地用户现在可以登录。

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。

暂时禁用并重新启用一个管理节点的 SSO

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

- 您拥有 "特定访问权限"。
- 您已获得 `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. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

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。