对StorageGRID 使用单点登录(SSO)

StorageGRID 11.5

NetApp
April 11, 2024

目录

对StorageGRID 使用单点登录(SSO)

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

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

单点登录的工作原理

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

启用SSO后登录

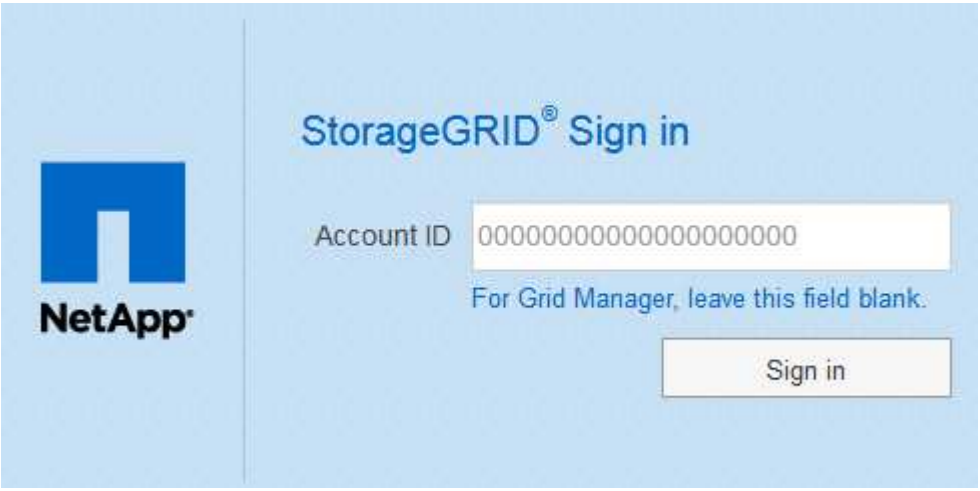
启用 SSO 并登录到 StorageGRID 后，系统会将您重定向到组织的 SSO 页面以验证您的凭据。

步骤

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

   此时将显示 StorageGRID 登录页面。

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

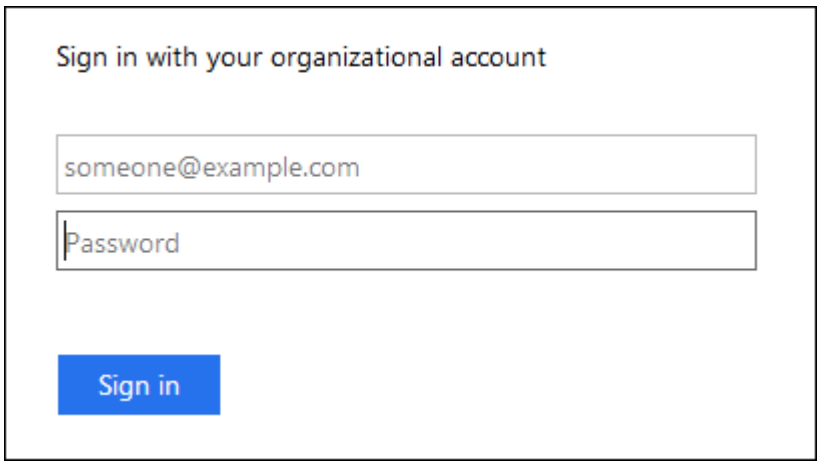


   - 如果您之前访问过网格管理器或租户管理器，系统将提示您选择最近的帐户或输入帐户 ID ：

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

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

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



4. 【签名 _sso]] 使用您的 SSO 凭据登录。

   如果您的 SSO 凭据正确：

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

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

   您无需重新输入 SSO 凭据。

启用SSO后注销

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

步骤

1. 找到用户界面右上角的 * 注销 * 链接。
2. 单击*注销*。

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

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

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

使用单点登录的要求

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

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

身份提供程序要求

用于SSO的身份提供程序(IdP)必须满足以下要求：

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

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

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

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

服务器证书要求

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

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

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

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

相关信息

"通过防火墙控制访问"

"为网格管理器和租户管理器配置自定义服务器证书"

配置单点登录

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

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

确认联合用户可以登录

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

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。

- 您必须具有特定的访问权限。
- 您正在使用Active Directory作为联合身份源、使用AD FS作为身份提供程序。

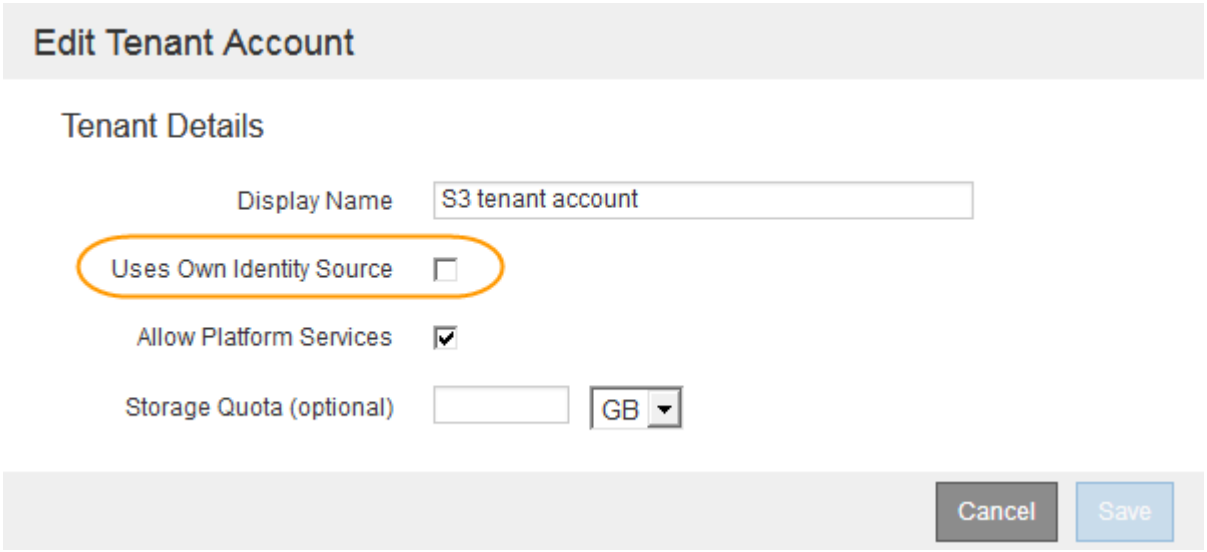
  "使用单点登录的要求"

步骤

1. 如果存在现有租户帐户，请确认所有租户均未使用其自己的身份源。

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

   a. 登录到每个租户帐户的租户管理器。
   b. 选择*访问控制*>*身份联合*。
   c. 确认未选中*启用身份联合*复选框。
   d. 如果是、请确认不再需要可能用于此租户帐户的任何联合组、取消选中此复选框、然后单击*保存*。
2. 确认联合用户可以访问网格管理器：
   a. 在网格管理器中、选择*配置*>*访问控制*>*管理组*。
   b. 确保已从Active Directory身份源导入至少一个联合组、并已为其分配"根访问"权限。
   c. 注销。
   d. 确认您可以以联合组中的用户身份重新登录到网格管理器。
3. 如果存在现有租户帐户、请确认具有root访问权限的联合用户可以登录：
   a. 在网格管理器中、选择*租户*。
   b. 选择租户帐户、然后单击*编辑帐户*。
   c. 如果选中了*使用自己的身份源*复选框、请取消选中该复选框、然后单击*保存*。



此时将显示租户帐户页面。

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

b. 在租户管理器中、单击*访问控制*>*组*。

c. 确保至少已为此租户为网格管理器中的一个联合组分配"根访问"权限。

d. 注销。

e. 确认您可以以联盟组中的用户身份重新登录到租户。

相关信息

"使用单点登录的要求"

"管理管理组"

"使用租户帐户"

使用沙盒模式

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

您需要的内容

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

关于此任务

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

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

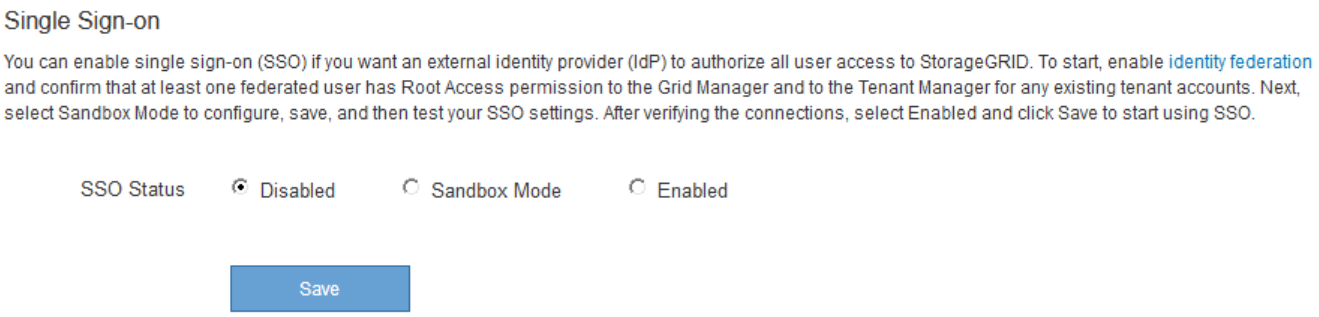
使用沙盒模式，可以轻松执行此背面配置，并在启用 SSO 之前测试所有设置。

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

步骤

1. 选择*配置访问控制单点登录*。

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



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

2. 选择*沙盒模式*选项。

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

3. 在身份提供程序部分中：

   a. 输入与AD FS中显示的名称完全相同的联合服务名称。

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

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

      - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
      - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

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

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

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

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

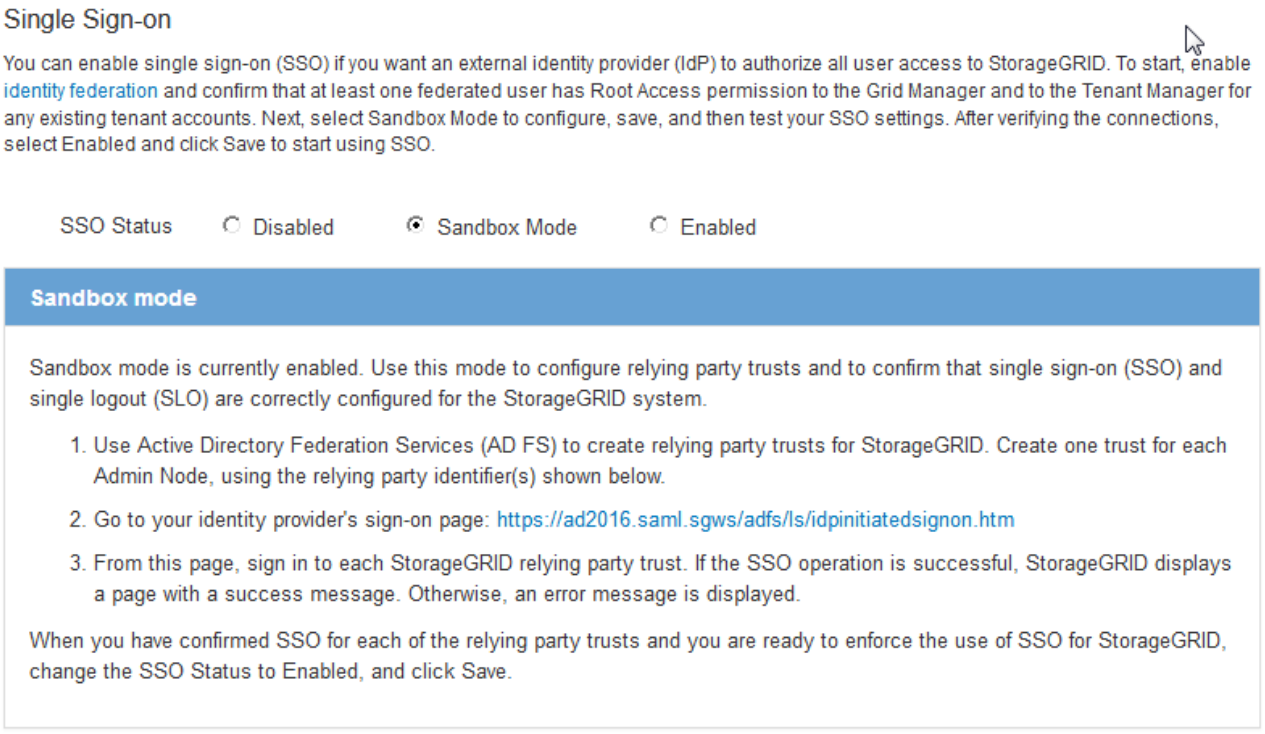
5. 单击 * 保存 * 。

   - 绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

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

赖方信任并测试单点登录(SSO)和单点注销(SLO)进程时使用此模式。



相关信息

"使用单点登录的要求"

在**AD FS**中创建依赖方信任

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

使用**Windows PowerShell**创建依赖方信任

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

您需要的内容

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

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

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

关于此任务

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

步骤

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

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

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

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

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

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

如果缺少元数据，请确认联合元数据地址是否正确，或者只需手动输入值即可。

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

通过导入联合元数据创建依赖方信任

您可以通过访问每个管理节点的 SAML 元数据来导入每个依赖方信任的值。

您需要的内容

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

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

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

关于此任务

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

步骤

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

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

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

6. 完成依赖方信任向导，保存依赖方信任并关闭该向导。

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

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

d. 在配置规则页面上，输入此规则的显示名称。

   例如，将 * 对象 GUID 更改为名称 ID* 。

e. 对于属性存储，选择 * Active Directory* 。

f. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。

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

h. 单击*完成*、然后单击*确定*。

8. 确认元数据已成功导入。

   a. 右键单击依赖方信任以打开其属性。

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

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

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

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

手动创建依赖方信任

如果您选择不导入依赖部件信任的数据，则可以手动输入值。

您需要的内容

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

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

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

关于此任务

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

步骤

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

   a. 输入此管理节点的显示名称。

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

b. 跳过此步骤可配置可选令牌加密证书。

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

d. 键入管理节点的 SAML 服务端点 URL：

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

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

e. 在配置标识符页面上，指定同一管理节点的依赖方标识符：

`Admin_Node_Identifier`

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

f. 查看设置，保存依赖方信任并关闭向导。

此时将显示编辑款项申请发放策略对话框。

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

6. 要启动声明规则向导、请单击*添加规则*：

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

b. 在配置规则页面上，输入此规则的显示名称。

例如，将 * 对象 GUID 更改为名称 ID* 。

c. 对于属性存储，选择 * Active Directory* 。

d. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。

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

f. 单击*完成*、然后单击*确定*。

7. 右键单击依赖方信任以打开其属性。

8. 在 * 端点 * 选项卡上，为单点注销（ SLO ）配置端点：

a. 单击*添加SAML *。

b. 选择 * 端点类型 * > * SAML 注销 * 。

c. 选择 * 绑定 * > * 重定向 * 。

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

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

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

a. 单击 * 确定 * 。

9. 在 * 签名 * 选项卡上，指定此依赖方信任的签名证书：

a. 添加自定义证书：

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

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

b. 单击*应用*、然后单击*确定*。

依赖方属性将被保存并关闭。

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

测试依赖方信任

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

您需要的内容

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

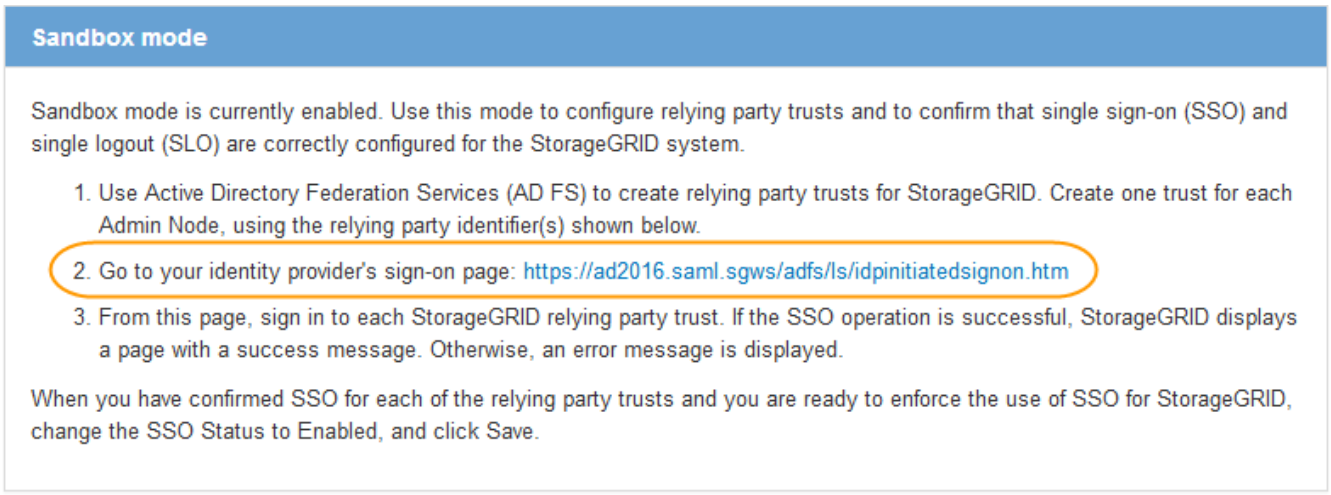
步骤

1. 选择*配置访问控制单点登录*。

此时将显示Single Sign-On页面、并选择了*沙盒模式*选项。

2. 在沙盒模式说明中、找到指向身份提供程序登录页面的链接。

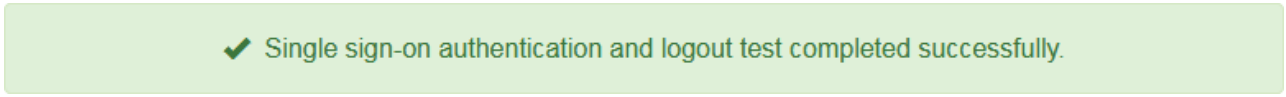
此URL是从您在*联合服务名称*字段中输入的值派生的。



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

系统将提示您输入用户名和密码。

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



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

如果所有SSO登录和注销操作均成功、则可以启用SSO。

启用单点登录

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

您需要的内容

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

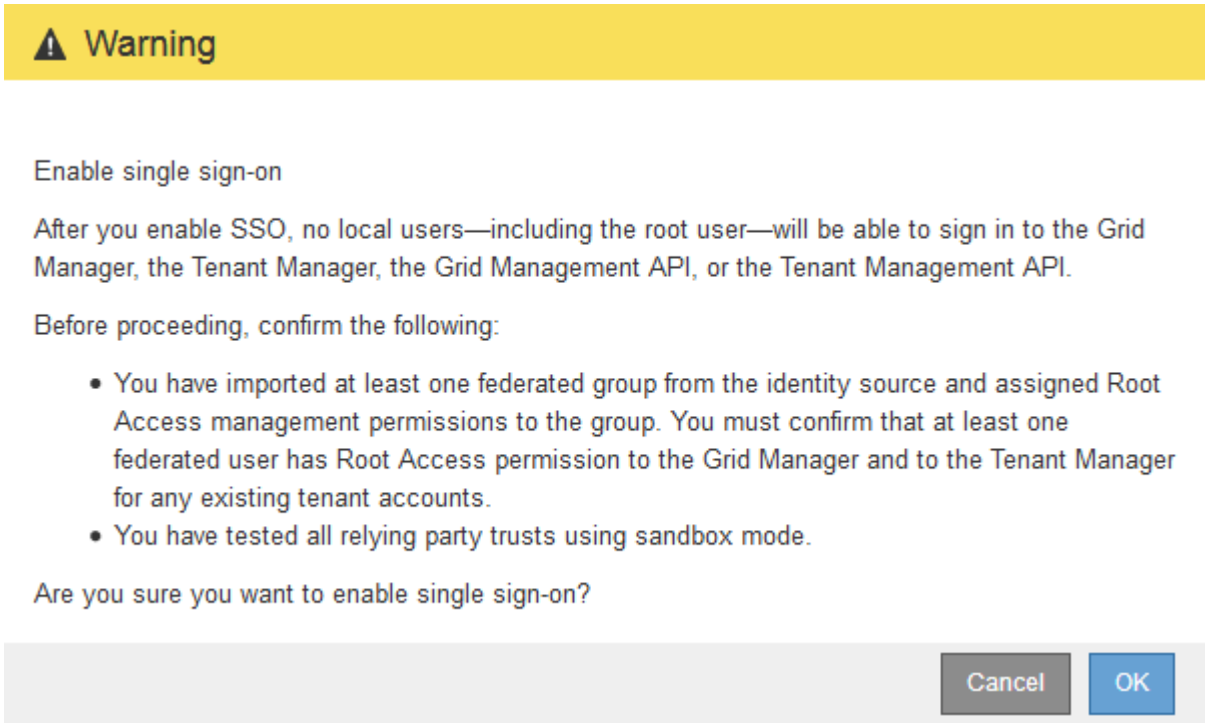
步骤

1. 选择*配置访问控制单点登录*。

   此时将显示Single Sign-On页面、并选择了*沙盒模式*。

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

   此时将显示一条警告消息。



4. 查看警告、然后单击*确定*。

   现在，已启用单点登录。

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

禁用单点登录

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

您需要的内容

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

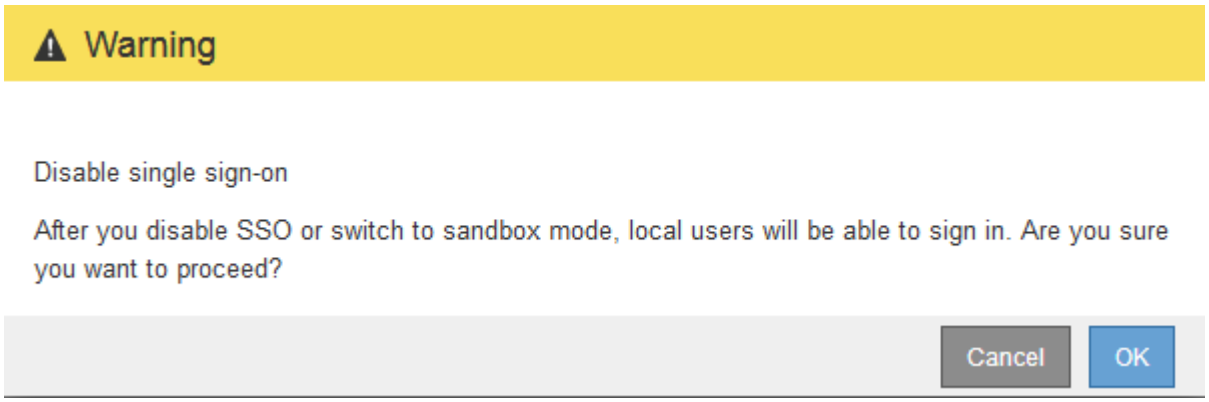
步骤

1. 选择*配置访问控制单点登录*。

   此时将显示 Single Sign-On 页面。

2. 选择 * 已禁用 * 选项。
3. 单击 * 保存 * 。

   此时将显示一条警告消息，指示本地用户现在可以登录。



4. 单击 * 确定 * 。

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

临时禁用并重新启用一个管理节点的单点登录

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

您需要的内容

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

关于此任务

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

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

步骤

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

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

2. 运行以下命令：`disable-saml`

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

3. 确认要禁用 SSO 。

   显示一条消息，指示节点上已禁用单点登录。

4. 从 Web 浏览器访问同一管理节点上的网格管理器。

   现在，由于已禁用 SSO ，将显示网格管理器登录页面。

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

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

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

      - 运行以下命令： `enable-saml`

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

      确认要启用 SSO 。

   显示一条消息，指示节点上已启用单点登录。

   - 重新启动网格节点： `reboot`

8. 从 Web 浏览器中，从同一管理节点访问网格管理器。

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

相关信息

"配置单点登录"