使用单点登录 (SSO)

StorageGRID software

NetApp
July 23, 2026

目录

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}