使用身份联合

StorageGRID 11.5

NetApp
April 11, 2024

目录

使用身份联合 1
配置联合身份源 1
强制与身份源同步 4
正在禁用身份联合 5

使用身份联合

使用身份联合可以加快租户组和用户的设置速度，并允许租户用户使用熟悉的凭据登录到租户帐户。

- "配置联合身份源"
- "强制与身份源同步"
- "正在禁用身份联合"

配置联合身份源

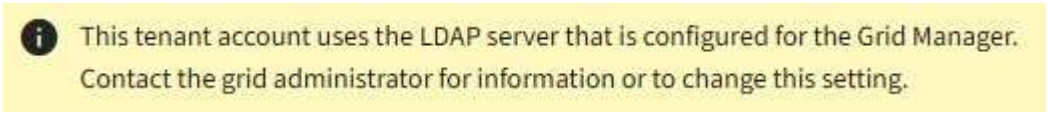
如果您希望在Active Directory、OpenLDAP或Oracle Directory Server等其他系统中管理租户组和用户、则可以配置身份联合。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有特定的访问权限。
- 您必须使用Active Directory、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、必须联系技术支持。
- 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，则身份提供程序必须使用 TLS 1.2 或 1.3 。

关于此任务

是否可以为租户配置身份联合服务取决于租户帐户的设置方式。您的租户可能会共享为网格管理器配置的身份联合服务。如果您在访问身份联合页面时看到此消息，则无法为此租户配置单独的联合身份源。



步骤

1. 选择 * 访问管理 * > * 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* Active Directory*、* OpenLDAP*或*其他*。

   如果选择* OpenLDAP*、请配置OpenLDAP服务器。请参见有关配置OpenLDAP服务器的准则。

   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。
   - * 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. 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服务器的服务器主机名或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
   - * 密码 * ： 与用户名关联的密码。
   - 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。

6. 在*传输层安全(TLS)*部分中、选择一个安全设置。
   - 使用**STARTTLS (**建议**)**：使用STARTTLS保护与LDAP服务器的通信安全。这是建议的选项。
   - * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。出于兼容性原因、支持此选项。
   - * 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。

     如果Active Directory服务器强制执行LDAP签名、则不支持此选项。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。

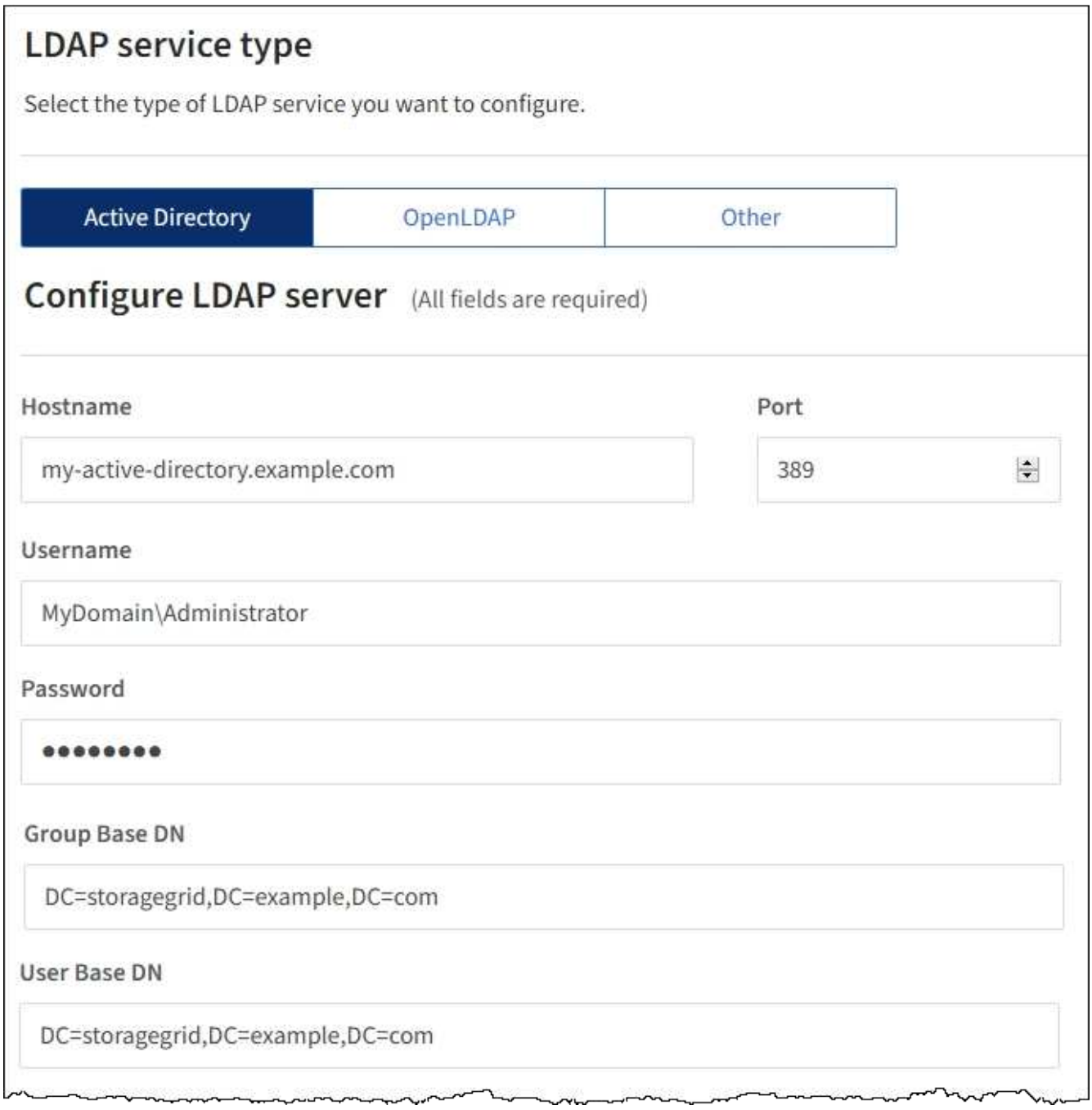
如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

8. 选择*测试连接*以验证LDAP服务器的连接设置。

   如果连接有效、页面右上角将显示一条确认消息。

9. 如果连接有效、请选择*保存*。

   以下屏幕截图显示了使用Active Directory的LDAP服务器的示例配置值。



相关信息

"租户管理权限"

"配置 OpenLDAP 服务器的准则"

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。

memberOf 和 **fint** 覆盖

应启用成员和精简覆盖。有关详细信息、请参见《OpenLDAP管理员指南》中有关反向组成员资格维护的说明。

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OpenLDAP管理员指南中有关反向组成员资格维护的信息。

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须具有特定的访问权限。
- 必须启用已保存的身份源。

步骤

1. 选择 * 访问管理 * > * 身份联合 * 。

   此时将显示"Identity Federation"页面。*同步服务器*按钮位于页面右上角。

   如果未启用保存的身份源、则*同步服务器*按钮将不会处于活动状态。

2. 选择*同步服务器*。

   此时将显示一条确认消息、指示同步已成功启动。

相关信息

"租户管理权限"

正在禁用身份联合

如果为此租户配置了身份联合服务、则可以临时或永久禁用租户组和用户的身份联合。禁用身份联合后、StorageGRID 系统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。

您需要的内容

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

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租户帐户的访问权限、直到其会话到期为止、但在会话到期后、他们将无法登录。
- StorageGRID 系统与身份源之间不会进行同步。

步骤

1. 选择 * 访问管理 * > * 身份联合 * 。
2. 取消选中*启用身份联合*复选框。
3. 选择 * 保存 * 。

相关信息

"租户管理权限"