管理群組和用戶

StorageGRID software

NetApp
May 29, 2026

目錄

管理群組和用戶

使用身分聯合

使用身分聯合可以更快地設定租用戶群組和用戶，並允許租用戶用戶使用熟悉的憑證登入租用戶帳戶。

為租用戶管理器配置身份聯合

如果您希望在另一個系統（例如 Active Directory、Azure Active Directory (Azure AD)、OpenLDAP 或 Oracle Directory Server）中管理租用戶群組和用戶，則可以為租用戶管理器設定身分聯合。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root存取權限"。
- 您正在使用 Active Directory、Azure AD、OpenLDAP 或 Oracle Directory Server 作為身分提供者。

  如果您想使用未列出的 LDAP v3 服務，請聯絡技術支援。

- 如果您打算使用 OpenLDAP，則必須設定 OpenLDAP 伺服器。看OpenLDAP 伺服器設定指南 。
- 如果您打算使用傳輸層安全性 (TLS) 與 LDAP 伺服器進行通信，則身分提供者必須使用 TLS 1.2 或 1.3。看"傳出 TLS 連線支援的密碼" 。

關於此任務

您是否可以為租用戶配置身分聯合服務取決於租用戶帳戶的設定方式。您的租戶可能會共用為網格管理器配置的身份聯合服務。如果您在造訪身分聯合頁面時看到此訊息，則表示您無法為此租用戶配置單獨的聯合身分識別來源。

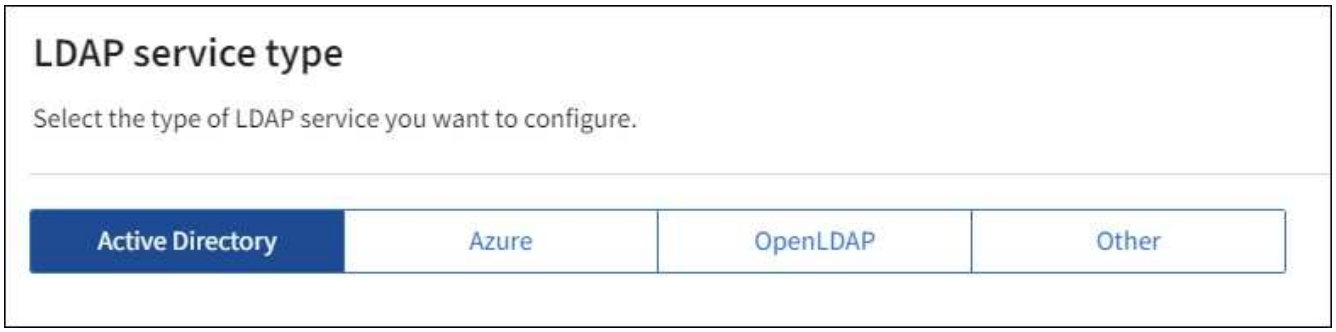
This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

輸入配置

設定身分聯合時，您需要提供StorageGRID連接到 LDAP 服務所需的值。

步驟

1. 選擇*存取管理* > 身分聯合。
2. 選擇*啟用身份聯合*。
3. 在 LDAP 服務類型部分中，選擇要設定的 LDAP 服務類型。



選擇「其他」來設定使用 Oracle Directory Server 的 LDAP 伺服器的值。

4. 如果您選擇了"其他"，請填寫 LDAP 屬性部分中的欄位。否則，轉到下一步。
   - 使用者唯一名稱：包含 LDAP 使用者唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName`對於 Active Directory 和 `uid`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `uid。
   - 使用者 **UUID**：包含 LDAP 使用者的永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID`對於 Active Directory 和 `entryUUID`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個使用者的指定屬性值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
   - 群組唯一名稱：包含 LDAP 群組唯一識別碼的屬性的名稱。此屬性相當於 `sAMAccountName`對於 Active Directory 和 `cn`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `cn。
   - 群組 **UUID**：包含 LDAP 群組的永久唯一識別碼的屬性的名稱。此屬性相當於 `objectGUID`對於 Active Directory 和 `entryUUID`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個群組的指定屬性的值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
5. 對於所有 LDAP 服務類型，請在設定 LDAP 伺服器部分輸入所需的 LDAP 伺服器和網路連線資訊。
   - 主機名稱：LDAP 伺服器的完全限定網域名稱 (FQDN) 或 IP 位址。
   - 連接埠：用於連接 LDAP 伺服器的連接埠。

     STARTTLS 的預設連接埠是 389，LDAPS 的預設連接埠是 636。但是，只要您的防火牆配置正確，您就可以使用任何連接埠。

   - 使用者名稱：將連接到 LDAP 伺服器的使用者的專有名稱 (DN) 的完整路徑。

     對於 Active Directory，您也可以指定下級登入名稱或使用者主體名稱。

     指定的使用者必須具有列出群組和使用者以及存取以下屬性的權限：

     - `sAMAccountName`或者 `uid`
     - `objectGUID`，`entryUUID`，或者 `nsuniqueid`
     - `cn`
     - `memberOf`或者 `isMemberOf`
     - 活動目錄：`objectSid`，`primaryGroupID`，`userAccountControl`，和 `userPrincipalName`

- 蔚藍： `accountEnabled`和 `userPrincipalName`

- 密碼：與使用者名稱關聯的密碼。

  如果您將來更改密碼，則必須在此頁面上更新。

- 群組基礎 **DN**：您要搜尋群組的 LDAP 子樹的可分辨名稱 (DN) 的完整路徑。在 Active Directory 範例（如下）中，所有可分辨名稱相對於基本 DN（DC=storagegrid、DC=example、DC=com）的群組都可以用作聯合群組。

  *群組唯一名稱*值在其所屬的*群組基本 DN*內必須是唯一的。

- 使用者基礎 **DN**：您要搜尋使用者的 LDAP 子樹的可分辨名稱 (DN) 的完整路徑。

  *使用者唯一名稱*值在其所屬的*使用者基本 DN*內必須是唯一的。

- 綁定使用者名稱格式（選用）：如果無法自動確定模式， StorageGRID應使用預設使用者名稱模式。

  建議提供*綁定使用者名稱格式*，因為如果StorageGRID無法與服務帳戶綁定，它可以允許使用者登入。

  輸入以下模式之一：

  - **UserPrincipalName** 模式（**Active Directory** 和 **Azure**）： `[USERNAME]@*example*.com`
  - 下級登入名稱模式（**Active Directory** 和 **Azure**）： `*example*\[USERNAME]`
  - 可分辨名稱模式： `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

    完全按照書寫方式包含 **[USERNAME]**。

6. 在傳輸層安全性 (TLS) 部分中，選擇一個安全性設定。

   - 使用 **STARTTLS**：使用 STARTTLS 確保與 LDAP 伺服器的通訊安全。這是 Active Directory、OpenLDAP 或其他的建議選項，但 Azure 不支援此選項。
   - 使用 **LDAPS**：LDAPS（透過 SSL 的 LDAP）選項使用 TLS 建立與 LDAP 伺服器的連線。您必須為 Azure 選擇此選項。
   - 請勿使用 **TLS**： StorageGRID系統和 LDAP 伺服器之間的網路流量將不安全。 Azure 不支援此選項。

     如果您的 Active Directory 伺服器強制執行 LDAP 簽名，則不支援使用 不使用 **TLS** 選項。您必須使用 STARTTLS 或 LDAPS。

7. 如果您選擇了 STARTTLS 或 LDAPS，請選擇用於保護連線的憑證。

   - 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 Grid CA 憑證來保護連線。
   - 使用自訂 **CA** 憑證：使用自訂安全性憑證。

     如果選擇此設置，請將自訂安全性憑證複製並貼上到 CA 憑證文字方塊中。

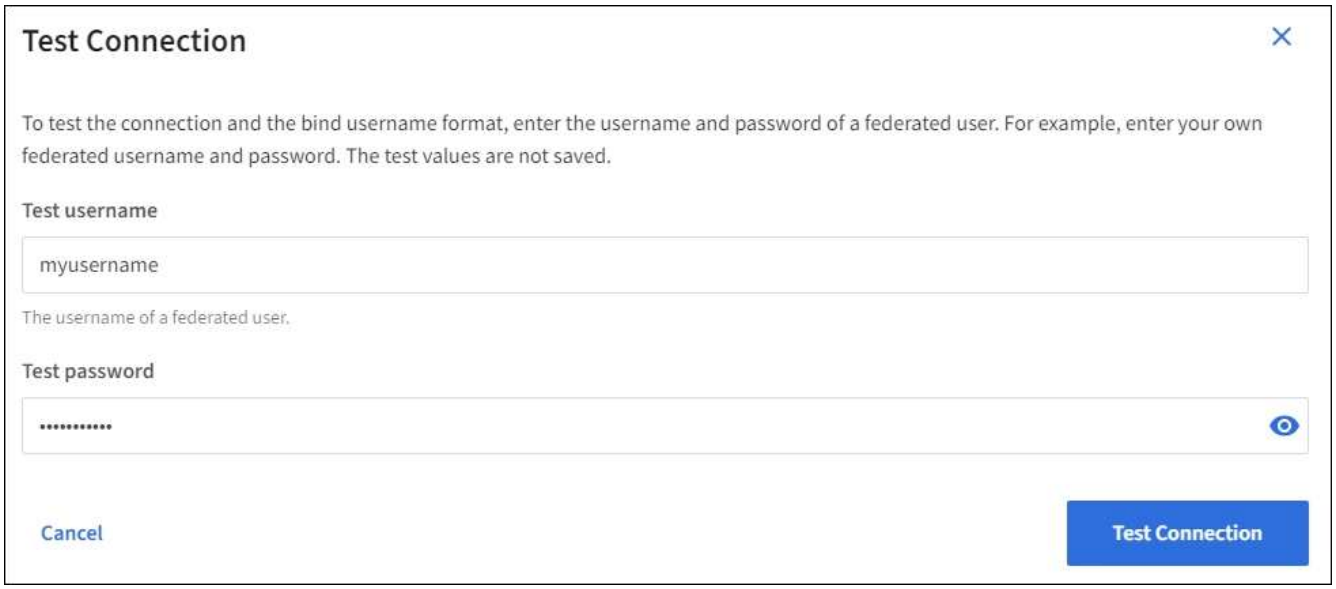
測試連接並儲存配置

輸入所有值後，必須先測試連接，然後才能儲存配置。如果您提供了 LDAP 伺服器的連線設定和綁定使用者名稱格式， StorageGRID會驗證該設定。

步驟

1. 選擇*測試連線*。
2. 如果您沒有提供綁定使用者名稱格式：
   - 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
   - 如果連線設定無效，則會出現「無法建立測試連線」訊息。選擇*關閉*。然後，解決所有問題並再次測試連線。
3. 如果您提供了綁定使用者名稱格式，請輸入有效聯合使用者的使用者名稱和密碼。

   例如，輸入您自己的使用者名稱和密碼。用戶名中不要包含任何特殊字符，例如 @ 或 /。



   - 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
   - 如果連線設定、綁定使用者名稱格式或測試使用者名稱和密碼無效，則會出現錯誤訊息。解決任何問題並再次測試連接。

強制與身分來源同步

StorageGRID系統會定期從身分識別來源同步聯合群組和使用者。如果您想盡快啟用或限制使用者權限，您可以強制啟動同步。

步驟

1. 前往身份聯合頁面。
2. 選擇頁面頂部的*同步伺服器*。

   同步過程可能需要一些時間，具體取決於您的環境。

   如果從身分來源同步聯合群組和使用者時出現問題，則會觸發*身分聯合同步失敗*警報。

禁用身份聯合

您可以暫時或永久停用群組和使用者的身份聯合。當身分聯合被停用時， StorageGRID和身分來源之間就沒有通訊。但是，您配置的任何設定都會保留，以便您將來可以輕鬆地重新啟用身份聯合。

關於此任務

在停用身分聯合之前，您應該注意以下事項：

- 聯合用戶將無法登入。
- 目前已登入的聯合用戶將保留對StorageGRID系統的存取權限，直到其會話過期，但會話過期後他們將無法登入。
- StorageGRID系統和身分來源之間不會發生同步，並且不會針對未同步的帳戶發出警報。
- 如果單一登入 (SSO) 設定為 已啟用 或 沙盒模式，則 啟用身分聯合 核取方塊將會停用。在停用身分聯合之前，單一登入頁面上的 SSO 狀態必須為 已停用。看"停用單一登入" 。

步驟

1. 前往身份聯合頁面。
2. 取消選取「啟用身份聯合」複選框。

OpenLDAP 伺服器設定指南

如果您想要使用 OpenLDAP 伺服器進行身份聯合，則必須在 OpenLDAP 伺服器上設定特定設定。

> 對於非 ActiveDirectory 或 Azure 的識別來源， StorageGRID不會自動阻止外部停用的使用者存取 S3。若要封鎖 S3 訪問，請刪除使用者的所有 S3 金鑰或從所有群組中刪除該使用者。

Memberof 和 refint 覆蓋

應該啟用 memberof 和 refint 覆蓋。有關詳細信息，請參閱http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文件：版本 2.4 管理員指南"^]。

索引

您必須使用指定的索引關鍵字來設定下列 OpenLDAP 屬性：

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

此外，請確保幫助中提到的使用者名字段已索引，以獲得最佳效能。

請參閱有關反向群組成員資格維護的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文件：版本 2.4 管理員指南"^]。

管理租戶群組

為 S3 租用戶建立群組

您可以透過匯入聯合群組或建立本機群組來管理 S3 使用者群組的權限。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root存取權限"。
- 如果您計劃匯入聯合群組，則必須"配置身份聯合"，且聯合群組已存在於配置的身份來源中。
- 如果您的租用戶帳戶具有「使用網格聯合連線」權限，則您已查看了下列工作流程和注意事項："克隆租戶群組和用戶" ，您已登入租戶的來源網格。

存取建立群組精靈

第一步，存取建立群組精靈。

步驟

1. 選擇*存取管理* > 群組。
2. 如果您的租用戶帳戶具有*使用網格聯合連線*權限，請確認出現藍色橫幅，表示在此網格上建立的新群組將被複製到連線中另一個網格上的相同租用戶。如果沒有出現此橫幅，您可能已登入租戶的目標網格。

3. 選擇*建立群組*。

選擇群組類型

您可以建立本機群組或匯入聯合群組。

步驟

1. 選擇「本機群組」標籤來建立本機群組，或選擇「聯合群組」標籤來從先前配置的身分來源匯入群組。

   如果您的StorageGRID系統啟用了單一登入 (SSO)，則屬於本機群組的使用者將無法登入租用戶管理器，但他們可以根據群組權限使用用戶端應用程式來管理租用戶的資源。

2. 輸入群組的名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後編輯顯示名稱。

     如果您的租用戶帳戶具有*使用網格聯合連線*權限，則當目標網格上已存在相同的租用戶*唯一名稱*時，將發生複製錯誤。

   - 聯合組：輸入唯一名稱。對於 Active Directory，唯一名稱是與 `sAMAccountName`屬性。對於 OpenLDAP，唯一名稱是與 `uid`屬性。
3. 選擇*繼續*。

管理群組權限

群組權限控制使用者可以在租用戶管理員和租用戶管理 API 中執行哪些任務。

步驟

1. 對於*存取模式*，請選擇以下之一：
   - 讀寫（預設）：使用者可以登入租用戶管理員並管理租用戶設定。
   - 只讀：使用者只能查看設定和功能。他們無法在租用戶管理員或租用戶管理 API 中進行任何變更或執行任何操作。本機只讀使用者可以更改自己的密碼。

     如果使用者屬於多個群組，並且任何群組設定為唯讀，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

2. 為此群組選擇一個或多個權限。

   看"租用戶管理權限" 。

3. 選擇*繼續*。

設定 **S3** 組策略

群組原則決定使用者將擁有哪些 S3 存取權限。

步驟

1. 選擇您想要用於該群組的策略。

群組原則	描述
無 S3 存取權限	預設.除非透過儲存桶策略授予存取權限，否則該群組中的使用者無權存取 S3 資源。如果選擇此選項，則預設只有 root 使用者才有權存取 S3 資源。
只讀訪問	此群組中的使用者對 S3 資源具有唯讀存取權限。例如，該群組中的使用者可以列出物件並讀取物件資料、元資料和標籤。選擇此選項時，唯讀群組原則的 JSON 字串將出現在文字方塊中。您無法編輯此字串。

群組原則	描述
完全存取權限	此群組中的使用者對 S3 資源（包括儲存桶）具有完全存取權限。當您選擇此選項時，完全存取群組原則的 JSON 字串將出現在文字方塊中。您無法編輯此字串。
勒索軟體緩解	此範例策略適用於此租用戶的所有儲存桶。該群組中的使用者可以執行常見操作，但無法從啟用了物件版本控制的儲存桶中永久刪除物件。 擁有「管理所有儲存桶」權限的租用戶管理員使用者可以覆寫此群組原則。將管理所有儲存桶的權限限制為受信任的用戶，並在可用的情況下使用多重身份驗證 (MFA)。
風俗	群組中的使用者被授予您在文字方塊中指定的權限。

2. 如果您選擇了*自訂*，請輸入群組原則。每個群組策略的大小限制為 5,120 位元組。您必須輸入有效的 JSON 格式的字串。

   有關群組策略的詳細資訊（包括語言語法和範例），請參閱"群組原則範例"。

3. 如果您正在建立本機群組，請選擇*繼續*。如果您正在建立聯合群組，請選擇*建立群組*和*完成*。

新增使用者（僅限本地群組）

您可以儲存群組而不新增用戶，也可以選擇新增任何已存在的本機用戶。

> 如果您的租用戶帳戶具有 使用網格聯合連接 權限，則在將群組複製到目標網格時，您在來源網格上建立本機群組時選擇的任何使用者都不會包括在內。因此，在創建群組時不要選擇使用者。相反，在建立使用者時選擇群組。

步驟

1. 或者，為此群組選擇一個或多個本機使用者。
2. 選擇*建立群組*和*完成*。

   您建立的群組將出現在群組清單中。

   如果您的租用戶帳戶具有*使用網格聯合連線*權限且您位於租用戶的來源網格上，則新群組將複製到租用戶的目標網格。 成功*在群組詳細資料頁面的概述部分中顯示為*克隆狀態。

為 **Swift** 租用戶建立群組

您可以透過匯入聯合群組或建立本機群組來管理 Swift 租用戶帳戶的存取權。至少一個群組必須具有 Swift 管理員權限，這是管理 Swift 租用戶帳戶的容器和物件所必需的。

> 對 Swift 用戶端應用程式的支援已被棄用，並將在未來的版本中刪除。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root存取權限"。
- 如果您計劃匯入聯合群組，則必須"配置身份聯合"，且聯合群組已存在於配置的身份來源中。

存取建立群組精靈

步驟

第一步，存取建立群組精靈。

1. 選擇*存取管理* > 群組。
2. 選擇*建立群組*。

選擇群組類型

您可以建立本機群組或匯入聯合群組。

步驟

1. 選擇「本機群組」標籤來建立本機群組，或選擇「聯合群組」標籤來從先前配置的身分來源匯入群組。

   如果您的StorageGRID系統啟用了單一登入 (SSO)，則屬於本機群組的使用者將無法登入租用戶管理器，但他們可以根據群組權限使用用戶端應用程式來管理租用戶的資源。

2. 輸入群組的名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後編輯顯示名稱。
   - 聯合組：輸入唯一名稱。對於 Active Directory，唯一名稱是與 `sAMAccountName`屬性。對於 OpenLDAP，唯一名稱是與 `uid`屬性。
3. 選擇*繼續*。

管理群組權限

群組權限控制使用者可以在租用戶管理員和租用戶管理 API 中執行哪些任務。

步驟

1. 對於*存取模式*，請選擇以下之一：
   - 讀寫（預設）：使用者可以登入租用戶管理員並管理租用戶設定。
   - 只讀：使用者只能查看設定和功能。他們無法在租用戶管理員或租用戶管理 API 中進行任何變更或執行任何操作。本機只讀使用者可以更改自己的密碼。

     如果使用者屬於多個群組，並且任何群組設定為唯讀，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

2. 如果群組使用者需要登入租用戶管理員或租用戶管理 API，請選取 **Root** 存取 複選框。
3. 選擇*繼續*。

設定 **Swift** 組策略

Swift 使用者需要管理員權限才能驗證 Swift REST API 來建立容器和提取物件。

1. 如果群組使用者需要使用 Swift REST API 來管理容器和對象，請選取 **Swift** 管理員 複選框。
2. 如果您正在建立本機群組，請選擇*繼續*。如果您正在建立聯合群組，請選擇*建立群組*和*完成*。

新增使用者（僅限本地群組）

您可以儲存群組而不新增用戶，也可以選擇新增任何已存在的本機用戶。

步驟

1. 或者，為此群組選擇一個或多個本機使用者。

   如果您尚未建立本機用戶，您可以在用戶頁面上將此群組新增至用戶。看"管理本地用戶" 。

2. 選擇*建立群組*和*完成*。

   您建立的群組將出現在群組清單中。

租用戶管理權限

在建立租用戶群組之前，請考慮要指派給該群組哪些權限。租用戶管理權限決定使用者可以使用租用戶管理員或租用戶管理 API 執行哪些任務。一個使用者可以屬於一個或多個群組。如果使用者屬於多個群組，則權限是累積的。

若要登入租用戶管理員或使用租用戶管理 API，使用者必須屬於具有至少一個權限的群組。所有可以登入的使用者都可以執行以下任務：

- 查看儀表板
- 更改自己的密碼（針對本機用戶）

對於所有權限，群組的存取模式設定決定使用者是否可以變更設定和執行操作，或者是否只能查看相關設定和功能。

> ⓘ 如果使用者屬於多個群組，並且任何群組設定為唯讀，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

您可以為群組指派以下權限。請注意，S3 租用戶和 Swift 租用戶具有不同的群組權限。

允許	描述	細節
Root 存取權限	提供對租用戶管理器和租用戶管理 API 的完全存取權。	Swift 使用者必須具有 Root 存取權限才能登入租用戶帳戶。
行政人員	僅限 Swift 租戶。提供此租用戶帳戶的 Swift 容器和物件的完全存取權限	Swift 使用者必須具有 Swift 管理員權限才能使用 Swift REST API 執行任何操作。

允許	描述	細節
管理您自己的 S3 憑證	允許使用者建立和刪除自己的 S3 存取密鑰。	沒有此權限的使用者看不到 儲存 **(S3)** > 我的 **S3** 存取金鑰 選單選項。
查看所有儲存桶	**S3** 租用戶：允許使用者查看所有儲存桶和儲存桶配置。 **Swift** 租用戶：允許 Swift 使用者使用租用戶管理 API 查看所有容器和容器配置。	沒有查看所有儲存桶或管理所有儲存桶權限的使用者看不到*儲存桶*選單選項。 此權限已被「管理所有儲存桶」權限取代。它不會影響 S3 用戶端或 S3 控制台使用的 S3 儲存桶或群組原則。 您只能從租用戶管理 API 將此權限指派給 Swift 群組。您不能使用租用戶管理員將此權限指派給 Swift 群組。
管理所有儲存桶	**S3** 租用戶：允許使用者使用租用戶管理器和租用戶管理 API 建立和刪除 S3 儲存桶，並管理租用戶帳戶中所有 S3 儲存桶的設置，而無需考慮 S3 儲存桶或群組原則。 **Swift** 租用戶：允許 Swift 使用者使用租用戶管理 API 控制 Swift 容器的一致性。	沒有查看所有儲存桶或管理所有儲存桶權限的使用者看不到*儲存桶*選單選項。 此權限取代了查看所有儲存桶的權限。它不會影響 S3 用戶端或 S3 控制台使用的 S3 儲存桶或群組原則。 您只能從租用戶管理 API 將此權限指派給 Swift 群組。您不能使用租用戶管理員將此權限指派給 Swift 群組。
管理端點	允許使用者使用租用戶管理器或租用戶管理 API 建立或編輯平台服務端點，這些端點用作StorageGRID平台服務的目標。	沒有此權限的使用者看不到*平台服務端點*選單選項。
使用 S3 控制台選項卡	與查看所有儲存桶或管理所有儲存桶權限結合使用時，可讓使用者從儲存桶詳細資料頁面上的 S3 控制台標籤檢視和管理物件。	

管理群組

根據需要管理您的租用戶群組，以查看、編輯或複製群組等。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root存取權限"。

檢視或編輯群組

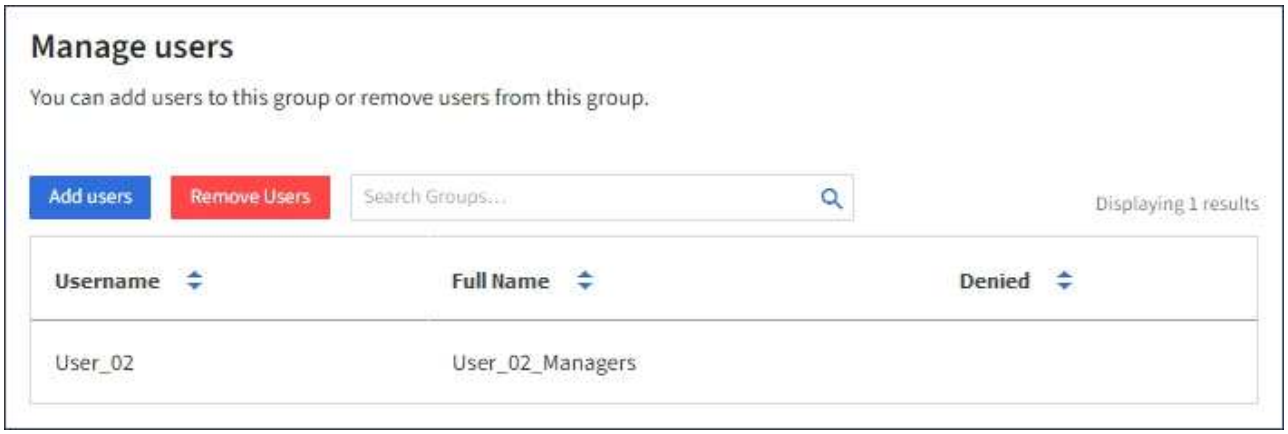
您可以查看和編輯每個群組的基本資訊和詳細資訊。

步驟

1. 選擇*存取管理* > 群組。
2. 查看「群組」頁面上提供的信息，其中列出了此租用戶帳戶的所有本機群組和聯合群組的基本資訊。

   如果租用戶帳戶具有 使用網格聯合連線 權限，並且您正在查看租用戶來源網格上的群組：

   - 橫幅訊息表明，如果您編輯或刪除一個群組，您的變更將不會同步到另一個網格。
   - 根據需要，橫幅訊息會指示群組是否未複製到目標網格上的租戶。你可以重試組克隆失敗了。
3. 如果您想要變更群組名稱：
   a. 選取該組的複選框。
   b. 選擇*操作* > 編輯群組名稱。
   c. 輸入新名稱。
   d. 選擇“儲存變更”。
4. 如果您想要查看更多詳細資訊或進行其他編輯，請執行以下操作之一：
   - 選擇組名。
   - 選取該群組的複選框，然後選擇*操作* > 查看群組詳細資訊。
5. 查看“概述”部分，其中顯示每個組的以下資訊：
   - 顯示名稱
   - 唯一名稱
   - 類型
   - 訪問模式
   - 權限
   - S3 策略
   - 本群組用戶數
   - 如果租用戶帳戶具有 使用網格聯合連線 權限且您正在查看租用戶來源網格上的群組，則附加欄位：
     - 克隆狀態，成功*或*失敗
     - 藍色橫幅表示如果您編輯或刪除該群組，您的變更將不會同步到其他網格。
6. 根據需要編輯群組設定。看"為 S3 租用戶建立群組"和"為 Swift 租用戶建立群組"了解輸入內容的詳細資訊。
   a. 在「概述」部分中，透過選擇名稱或編輯圖標。
   b. 在*群組權限*標籤上，更新權限，然後選擇*儲存變更*。
   c. 在「群組原則」標籤上進行任何更改，然後選擇「儲存變更」。
      - 如果您正在編輯 S3 群組，則可以根據需要選擇不同的 S3 群組原則或輸入自訂策略的 JSON 字串。
      - 如果您正在編輯 Swift 群組，可以選擇或清除 **Swift** 管理員 複選框。
7. 若要將一個或多個現有本機使用者新增至群組：
   a. 選擇“用戶”選項卡。



b. 選擇*新增使用者*。

c. 選擇您想要新增的現有用戶，然後選擇*新增用戶*。

右上角會出現成功訊息。

8. 若要從群組中刪除本機使用者：

a. 選擇“用戶”選項卡。

b. 選擇*刪除使用者*。

c. 選擇要刪除的用戶，然後選擇*刪除用戶*。

右上角會出現成功訊息。

9. 確認您為變更的每個部分選擇了「儲存變更」。

重複組

您可以複製現有群組以更快地建立新群組。

如果您的租用戶帳戶具有*使用網格聯合連線*權限，並且您從租用戶的來源網格複製一個群組，則複製的群組將被複製到租戶的目標網格。

步驟

1. 選擇*存取管理* > 群組。
2. 選取要複製的群組的複選框。
3. 選擇*動作* > 複製群組。
4. 看"為 S3 租用戶建立群組"或者"為 Swift 租用戶建立群組"了解輸入內容的詳細資訊。
5. 選擇*建立群組*。

重試組克隆

要重試失敗的克隆：

1. 選擇群組名稱下方指示「（克隆失敗）」的每個群組。
2. 選擇*操作* > 克隆組。

3. 從您正在複製的每個群組的詳細資訊頁面查看克隆操作的狀態。

有關更多信息，請參閱"克隆租戶群組和用戶"。

刪除一個或多個群組

您可以刪除一個或多個群組。任何僅屬於已刪除群組的使用者將不再能夠登入租用戶管理員或使用租用戶帳戶。

> 如果您的租用戶帳戶具有*使用網格聯合連線*權限並且您刪除了一個群組， StorageGRID將不會刪除另一個網格上的相應群組。如果您需要保持此資訊同步，則必須從兩個網格中刪除相同的群組。

步驟

1. 選擇*存取管理* > 群組。
2. 選取要刪除的每個群組的複選框。
3. 選擇*動作* > 刪除群組*或*操作 > 刪除群組。

   出現確認對話框。

4. 選擇*刪除群組*或*刪除群組*。

管理本地用戶

您可以建立本機使用者並將他們指派到本機群組，以確定這些使用者可以存取哪些功能。租用戶管理器包括一個名為「root」的預先定義本機使用者。雖然您可以新增和刪除本機用戶，但您無法刪除根用戶。

> 如果您的StorageGRID系統啟用了單一登入 (SSO)，本機使用者將無法登入租用戶管理器或租用戶管理 API，但他們可以根據群組權限使用用戶端應用程式存取租用戶的資源。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root存取權限"。
- 如果您的租用戶帳戶具有「使用網格聯合連線」權限，則您已查看了下列工作流程和注意事項："克隆租戶群組和用戶" ，您已登入租戶的來源網格。

建立本機用戶

您可以建立本機使用者並將其指派給一個或多個本機群組以控制他們的存取權限。

不屬於任何群組的 S3 使用者沒有管理權限或不套用 S3 群組原則。這些使用者可能透過儲存桶策略取得 S3 儲存桶存取權限。

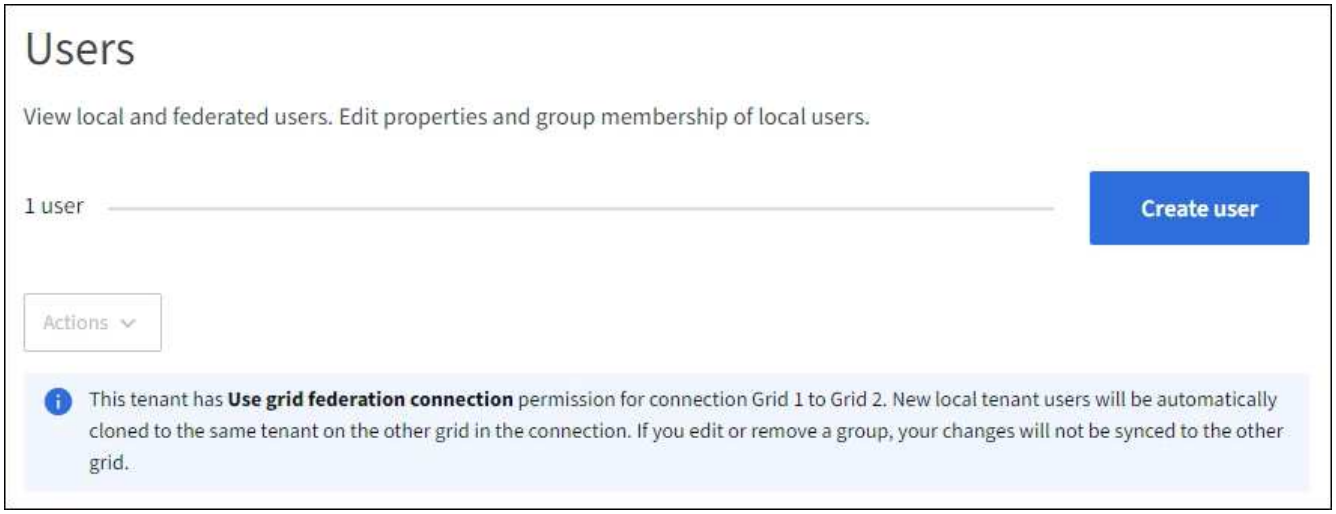
不屬於任何群組的 Swift 使用者沒有管理權限或 Swift 容器存取權限。

存取建立使用者精靈

步驟

1. 選擇*存取管理* > 使用者。

   如果您的租用戶帳戶具有*使用網格聯合連線*權限，則藍色橫幅表示這是租用戶的來源網格。您在此網格上建立的任何本機使用者都會被複製到連接中的另一個網格。



2. 選擇*建立使用者*。

輸入憑證

步驟

1. 對於*輸入使用者憑證*步驟，請填寫以下欄位。

場地	描述
姓名	此使用者的全名，例如，一個人的名字和姓氏或應用程式的名稱。
使用者名稱	此用戶將用於登入的名稱。使用者名稱必須是唯一的，並且不能更改。 注意：如果您的租用戶帳戶具有*使用網格聯合連線*權限，則當目標網格上已存在與該租用戶相同的*使用者名稱*時，將發生複製錯誤。
密碼和確認密碼	使用者最初登入時所使用的密碼。
拒絕訪問	選擇「是」可阻止該使用者登入租用戶帳戶，即使他們可能仍屬於一個或多個群組。 例如，選擇「是」可暫時中止使用者的登入權限。

2. 選擇*繼續*。

分配給群組

步驟

1. 將使用者指派到一個或多個本地群組以確定他們可以執行哪些任務。

   將使用者指派到群組是可選的。如果您願意，您可以在建立或編輯群組時選擇使用者。

   不屬於任何群組的使用者將沒有管理權限。權限是累積的。使用者將擁有其所屬的所有群組的所有權限。看"租用戶管理權限" 。

2. 選擇*建立使用者*。

   如果您的租用戶帳戶具有*使用網格聯合連線*權限且您位於租用戶的來源網格上，則新的本機使用者將被複製到租用戶的目標網格。 成功*在使用者詳細資料頁面的概覽部分中顯示為*克隆狀態。

3. 選擇“完成”返回“使用者”頁面。

查看或編輯本機用戶

步驟

1. 選擇*存取管理* > 使用者。
2. 查看「使用者」頁面上提供的信息，其中列出了此租戶帳戶的所有本地用戶和聯合用戶的基本資訊。

   如果租用戶帳戶具有 使用網格聯合連線 權限，且您正在查看租用戶來源網格上的使用者：

   - 橫幅訊息表明，如果您編輯或刪除用戶，您的變更將不會同步到另一個網格。
   - 根據需要，橫幅訊息會指示使用者是否未複製到目標網格上的租戶。您可以重試失敗的用戶克隆 。

3. 如果要更改使用者的全名：
   a. 選取使用者的複選框。
   b. 選擇*動作* > 編輯全名。
   c. 輸入新名稱。
   d. 選擇“儲存變更”。
4. 如果您想要查看更多詳細資訊或進行其他編輯，請執行以下操作之一：
   - 選擇用戶名。
   - 選取使用者的複選框，然後選擇*操作* > 查看使用者詳細資料。
5. 查看“概述”部分，其中顯示每個用戶的以下資訊：
   - 姓名
   - 使用者名稱
   - 使用者類型
   - 拒絕訪問
   - 訪問模式
   - 團體成員資格

- 如果租用戶帳戶具有 使用網格聯合連線 權限且您正在租用戶的來源網格上檢視用戶，則附加欄位：
  - 克隆狀態，成功*或*失敗
  - 藍色橫幅表示如果您編輯此用戶，您的變更將不會同步到其他網格。

6. 根據需要編輯用戶設定。看建立本地用戶了解輸入內容的詳細資訊。
   a. 在「概述」部分中，透過選擇名稱或編輯圖示來變更全名。

      您不能更改使用者名稱。

   b. 在*密碼*標籤上，變更使用者密碼，然後選擇*儲存變更*。
   c. 在「存取」標籤上，選擇「否」以允許使用者登錄，或選擇「是」以阻止使用者登入。然後，選擇“儲存變更”。
   d. 在「存取金鑰」標籤上，選擇「建立金鑰」並按照指示進行操作"建立另一個使用者的 S3 存取金鑰"。
   e. 在「群組」標籤上，選擇「編輯群組」將使用者新增至群組或從群組中刪除使用者。然後，選擇*儲存變更*。
7. 確認您為變更的每個部分選擇了「儲存變更」。

重複的本地用戶

您可以複製本機使用者以更快地建立新使用者。

> 如果您的租用戶帳戶具有*使用網格聯合連線*權限，並且您從租用戶的來源網格複製用戶，則重複的用戶將被複製到租用戶的目標網格。

步驟

1. 選擇*存取管理* > 使用者。
2. 選取您想要複製的使用者的複選框。
3. 選擇*動作* > 重複使用者。
4. 看建立本地用戶了解輸入內容的詳細資訊。
5. 選擇*建立使用者*。

重試用戶克隆

要重試失敗的克隆：

1. 選擇用戶名下方標有“（克隆失敗）”的每個用戶。
2. 選擇*操作* > 複製使用者。
3. 從您正在複製的每個使用者的詳細資訊頁面查看克隆操作的狀態。

有關更多信息，請參閱"克隆租戶群組和用戶"。

刪除一個或多個本機用戶

您可以永久刪除一個或多個不再需要存取StorageGRID租用戶帳戶的本機使用者。

如果您的租用戶帳戶具有*使用網格聯合連線*權限並且您刪除本機用戶，則StorageGRID將不會刪除另一個網格上的對應用戶。如果您需要保持此資訊同步，則必須從兩個網格中刪除同一個使用者。

您必須使用聯合身份來源來刪除聯合使用者。

步驟

1. 選擇*存取管理* > 使用者。
2. 選取要刪除的每個使用者的複選框。
3. 選擇*操作* > 刪除使用者*或*操作 > 刪除使用者。

   出現確認對話框。

4. 選擇*刪除使用者*或*刪除使用者*。