管理群組和使用者

StorageGRID 11.7

NetApp
April 12, 2024

目錄

管理群組和使用者

使用身分識別聯盟

使用身分識別聯盟可更快設定租戶群組和使用者、並可讓租戶使用者使用熟悉的認證登入租戶帳戶。

設定租戶管理程式的身分識別聯盟

如果您想要在其他系統（例如Active Directory、Azure Active Directory（Azure AD）、OpenLDAP或Oracle Directory Server）中管理租戶群組和使用者、可以為租戶管理程式設定身分識別聯盟。

開始之前

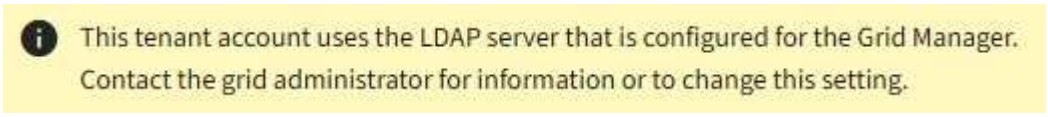
- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 您使用Active Directory、Azure AD、OpenLDAP或Oracle Directory Server做為身分識別供應商。

  如果您想使用未列出的LDAP v3服務、請聯絡技術支援部門。

- 如果您打算使用OpenLDAP、則必須設定OpenLDAP伺服器。請參閱 設定OpenLDAP伺服器的準則。
- 如果您打算使用傳輸層安全性（TLS）與LDAP伺服器進行通訊、則身分識別供應商必須使用TLS 1.2或1.3。請參閱 "用於傳出TLS連線的支援密碼"。

關於這項工作

您是否可以為租戶設定身分識別聯盟服務、取決於租戶帳戶的設定方式。您的租戶可能會共用為Grid Manager設定的身分識別聯盟服務。如果您在存取「身分識別聯盟」頁面時看到此訊息、則無法為此租用戶設定個別的同盟身分識別來源。

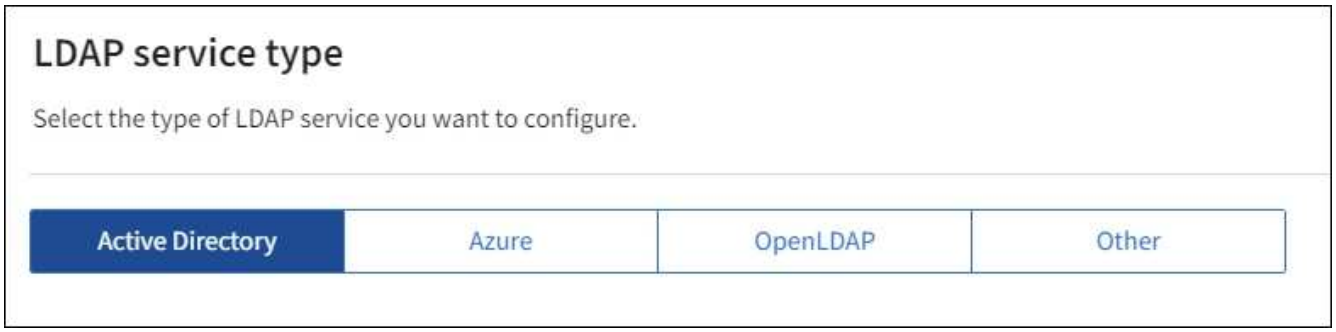


輸入組態

當您設定識別聯盟時、您會提供 StorageGRID 連線至 LDAP 服務所需的值。

步驟

1. 選擇*存取管理*>*身分識別聯盟*。
2. 選取*啟用身分識別聯盟*。
3. 在LDAP服務類型區段中、選取您要設定的LDAP服務類型。



選擇*其他*以設定使用Oracle Directory Server的LDAP伺服器值。

4. 如果選擇*其他*、請填寫「LDAP屬性」區段中的欄位。否則、請前往下一步。
   - 使用者唯一名稱：含有LDAP使用者唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName` 適用於Active Directory和 `uid` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `uid`。
   - *使用者UUID *：含有LDAP使用者永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `nsuniqueid`。指定屬性的每個使用者值必須是16位元組或字串格式的32位數十六進位數字、連字號會被忽略。
   - 群組唯一名稱：包含LDAP群組唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName` 適用於Active Directory和 `cn` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `cn`。
   - *群組UUID *：包含LDAP群組永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `nsuniqueid`。指定屬性的每個群組值必須是16位元組或字串格式的32位數十六進位數字、連字號會被忽略。
5. 對於所有LDAP服務類型、請在「設定LDAP伺服器」區段中輸入所需的LDAP伺服器和網路連線資訊。
   - 主機名稱：LDAP伺服器的完整網域名稱（FQDN）或IP位址。
   - 連接埠：用於連接LDAP伺服器的連接埠。

     STARTTLS的預設連接埠為389、LDAPS的預設連接埠為636。不過、只要防火牆設定正確、您就可以使用任何連接埠。

   - 使用者名稱：將連線至LDAP伺服器之使用者的辨別名稱（DN）完整路徑。

     對於Active Directory、您也可以指定低層級的登入名稱或使用者主要名稱。

     指定的使用者必須擁有列出群組和使用者的權限、並可存取下列屬性：

     - `sAMAccountName` 或 `uid`
     - `objectGUID`、 `entryUUID`或 `nsuniqueid`
     - `cn`
     - `memberOf` 或 `isMemberOf`
     - * Active Directory* ： `objectSid`、 `primaryGroupID`、 `userAccountControl`和 `userPrincipalName`
     - * Azure * ： `accountEnabled` 和 `userPrincipalName`

- 密碼：與使用者名稱相關的密碼。
- 群組基礎**DN**：您要搜尋群組之LDAP子樹狀結構的辨別名稱（DN）完整路徑。在Active Directory範例（如下）中、識別名稱相對於基礎DN（DC=storagegRID、DC=example、DC=com）的所有群組均可做為聯盟群組使用。

  「群組唯一名稱*」值必須在所屬的*群組基礎DN*中是唯一的。

- 使用者基礎**DN**：您要搜尋使用者之LDAP子樹狀目錄的辨別名稱（DN）完整路徑。

  *使用者唯一名稱*值必須在其所屬的*使用者基礎DN*內是唯一的。

- * 連結使用者名稱格式 * （選用）：如果無法自動判斷模式、則應使用預設的使用者名稱模式StorageGRID 。

  建議提供*連結使用者名稱格式*、因為StorageGRID 如果無法連結服務帳戶、使用者可以登入。

  輸入下列其中一種模式：

  - * UserPrincipalName 模式（ Active Directory 和 Azure ） * ： `[USERNAME]@example.com`
  - * 低階登入名稱模式（ Active Directory 和 Azure ） * ： `example\[USERNAME]`
  - * 辨別名稱模式 * ： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    請準確附上所寫的*（使用者名稱）*。

6. 在傳輸層安全性（TLS）區段中、選取安全性設定。
   - 使用**ARTTLS**：使用ARTTLS來保護與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（LDAP over SSL）選項使用TLS建立與LDAP伺服器的連線。您必須為Azure選取此選項。
   - 請勿使用**TLS**：StorageGRID 不保護介於整個系統與LDAP伺服器之間的網路流量。Azure不支援此選項。

     如果Active Directory伺服器強制執行LDAP簽署、則不支援使用*「不使用TLS*」選項。您必須使用ARTTLS或LDAPS。

7. 如果您選取了ARTTLS或LDAPS、請選擇用來保護連線安全的憑證。
   - 使用作業系統**CA**憑證：使用作業系統上安裝的預設Grid CA憑證來保護連線安全。
   - 使用自訂**CA**憑證：使用自訂安全性憑證。

     如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

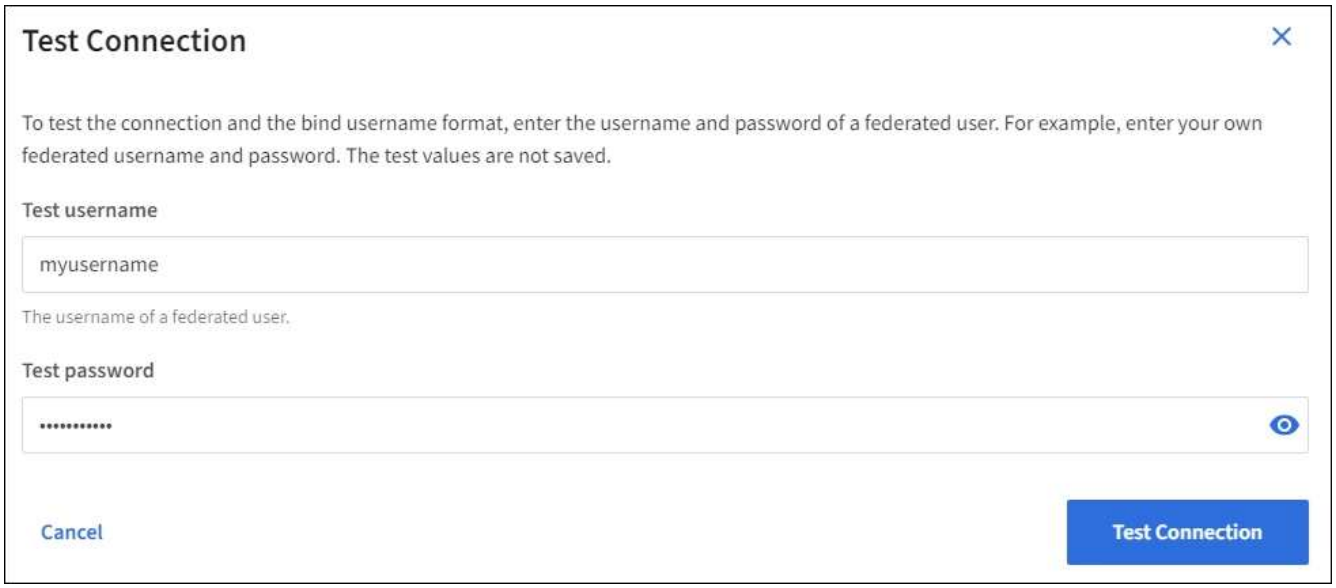
測試連線並儲存組態

輸入所有值之後、您必須先測試連線、才能儲存組態。如果您提供LDAP伺服器的連線設定和連結使用者名稱格式、則可透過此驗證。StorageGRID

步驟

1. 選擇*測試連線*。
2. 如果您未提供連結使用者名稱格式：
   - 如果連線設定有效、則會出現「Test connection Successful（測試連線成功）」訊息。選取*「Save（儲存）」*以儲存組態。
   - 如果連線設定無效、則會出現「test connection Could not be connection…（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. 如果您提供連結使用者名稱格式、請輸入有效同盟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。請勿在使用者名稱中包含任何特殊字元、例如 @ 或 / 。



   - 如果連線設定有效、則會出現「Test connection Successful（測試連線成功）」訊息。選取*「Save（儲存）」*以儲存組態。
   - 如果連線設定、連結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。解決所有問題、然後再次測試連線。

強制與身分識別來源同步

此系統會定期同步來自身分識別來源的聯盟群組和使用者。StorageGRID如果您想要盡快啟用或限制使用者權限、可以強制啟動同步。

步驟

1. 前往「身分識別聯盟」頁面。
2. 選取頁面頂端的*同步伺服器*。

   視您的環境而定、同步處理程序可能需要一些時間。

   如果同步處理來自身分識別來源的聯盟群組和使用者時發生問題、則會觸發*身分識別聯盟同步處理失敗*警示。

停用身分識別聯盟

您可以暫時或永久停用群組和使用者的身分識別聯盟。停用身分識別聯盟時StorageGRID 、不會在驗證和身分識別來源之間進行通訊。不過、您已設定的任何設定都會保留下來、讓您日後可以輕鬆重新啟用身分識別聯盟。

關於這項工作

在停用身分識別聯盟之前、您應注意下列事項：

- 聯盟使用者將無法登入。
- 目前已登入的聯盟使用者將在StorageGRID 其工作階段過期之前保留對此系統的存取權、但在工作階段過期後仍無法登入。
- 不會在不同步系統與身分識別來源之間進行同步、StorageGRID 也不會針對尚未同步的帳戶發出警示或警示。
- 如果將單點登錄 (SSO) 設置爲 **Enabled** 或 **Sandbox Mode** ，則禁用 **Enable identity Federation** （啓用身份聯合） * 複選框。「單一登入」頁面的**SSO**狀態必須為*停用、才能停用身分識別聯盟。請參閱 "停用單一登入"。

步驟

1. 前往「身分識別聯盟」頁面。
2. 取消勾選 * 啟用身分識別聯盟 * 核取方塊。

設定**OpenLDAP**伺服器的準則

如果您要使用OpenLDAP伺服器進行身分識別聯盟、則必須在OpenLDAP伺服器上設定特定設定。

> 對於非 ActiveDirectory 或 Azure 的身分識別來源、 StorageGRID 不會自動封鎖 S3 對外部停用使用者的存取。若要封鎖 S3 存取、請刪除使用者的任何 S3 金鑰、或將使用者從所有群組中移除。

memberOf和**refert**覆疊

應啟用memberof和refert覆疊。如需詳細資訊、請參閱中的反轉群組成員資格維護指示http://www.openldap.org/doc/admin24/index.html["OpenLDAP文件：2.4版管理員指南"^]。

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、請確定使用者名稱說明中所述的欄位已建立索引、以獲得最佳效能。

請參閱中有關反轉群組成員資格維護的資訊http://www.openldap.org/doc/admin24/index.html["OpenLDAP文件：2.4版管理員指南"^]。

管理租戶群組

為S3租戶建立群組

您可以匯入同盟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

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 如果您計畫匯入同盟群組、您就擁有了 "已設定的身分識別聯盟"，且已設定的身分識別來源中已存在同盟群組。
- 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、您已檢閱的工作流程和考量事項 "複製租戶群組和使用者"，您將登入租戶的來源網格。

存取建立群組精靈

第一步是存取「建立群組」精靈。

步驟

1. 選擇*存取管理*>*群組*。
2. 如果您的租戶帳戶具有 * 使用網格同盟連線 * 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會複製到連線中其他網格上的同一個租戶。如果未顯示此橫幅、您可能會登入租戶的目的地網格。

3. 選取*建立群組*。

選擇群組類型

您可以建立本機群組或匯入同盟群組。

步驟

1. 選取*本機群組*索引標籤以建立本機群組、或選取*聯盟群組*索引標籤、從先前設定的身分識別來源匯入群組。

   如果StorageGRID 您的系統啟用單一登入（SSO）、屬於本機群組的使用者將無法登入租戶管理程式、不

過他們可以根據群組權限、使用用戶端應用程式來管理租戶的資源。

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

     如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則如果目的地網格上的租戶已經存在相同的 * 唯一名稱 * 、就會發生複製錯誤。

   - 聯盟群組：輸入唯一名稱。對於Active Directory、唯一名稱是與相關聯的名稱 `sAMAccountName` 屬性。對於OpenLDAP、唯一名稱是與相關聯的名稱 `uid` 屬性。
3. 選擇*繼續*。

管理群組權限

群組權限可控制使用者可在租戶管理器和租戶管理 API 中執行的工作。

步驟

1. 對於 * 存取模式 * 、請選取下列其中一項：
   - * 讀寫 *（預設）：使用者可以登入租戶管理員並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。他們無法在租戶管理員或租戶管理 API 中進行任何變更或執行任何作業。本機唯讀使用者可以變更自己的密碼。

     如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。

2. 為此群組選取一或多個權限。

   請參閱 "租戶管理權限"。

3. 選擇*繼續*。

設定 **S3** 群組原則

群組原則決定使用者將擁有哪些 S3 存取權限。

步驟

1. 選取您要用於此群組的原則。

群組原則	說明
無 S3 存取權	預設。此群組中的使用者無法存取 S3 資源、除非已透過貯體原則授予存取權限。如果選取此選項、預設只有root使用者可以存取S3資源。
唯讀存取	此群組中的使用者擁有 S3 資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。

群組原則	說明
完整存取	此群組中的使用者可完全存取 S3 資源、包括貯體。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
勒索軟體緩解	此範例原則適用於此租戶的所有貯體。此群組中的使用者可以執行一般動作、但無法從已啟用物件版本設定的儲存區中永久刪除物件。 擁有「 * 管理所有儲存區 * 」權限的租戶管理員使用者可以覆寫此群組原則。將「管理所有貯體」權限限制於信任的使用者、並在可行的情況下使用「多因素驗證」（ MFA ）。
自訂	群組中的使用者會獲得您在文字方塊中指定的權限。

2. 如果您選取*自訂*、請輸入群組原則。每個群組原則的大小上限為5、120位元組。您必須輸入有效的Json格式字串。

   如需群組原則的詳細資訊、包括語言語法和範例、請參閱 "群組原則範例"。

3. 如果您要建立本機群組、請選取*繼續*。如果您要建立聯盟群組、請選取*建立群組*和*完成*。

新增使用者（僅限本機群組）

您可以儲存群組而不新增使用者、也可以選擇性地新增已存在的任何本機使用者。

> 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則當您在來源網格上建立本機群組時、所選取的任何使用者、都不會被複製到目的地網格時納入。因此、建立群組時請勿選取使用者。而是在建立使用者時選取群組。

步驟

1. 您也可以為此群組選取一或多個本機使用者。
2. 選擇* Create group（創建組）和 Finish（完成）*。

   您建立的群組會出現在群組清單中。

   如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您位於租戶的來源網格上、則新群組會複製到租戶的目的地網格。* 成功 * 會在群組詳細資料頁面的「概述」區段中顯示為 * 複製狀態 * 。

為Swift租戶建立群組

您可以匯入聯盟群組或建立本機群組、來管理Swift租戶帳戶的存取權限。至少一個群組必須具有Swift Administrator權限、這是管理Swift租戶帳戶的容器和物件所需的權限。

> Swift 用戶端應用程式的支援已過時、未來版本將會移除。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 如果您計畫匯入同盟群組、您就擁有了 "已設定的身分識別聯盟"，且已設定的身分識別來源中已存在同盟群組。

存取建立群組精靈

步驟

第一步是存取「建立群組」精靈。

1. 選擇*存取管理*>*群組*。
2. 選取*建立群組*。

選擇群組類型

您可以建立本機群組或匯入同盟群組。

步驟

1. 選取*本機群組*索引標籤以建立本機群組、或選取*聯盟群組*索引標籤、從先前設定的身分識別來源匯入群組。

   如果StorageGRID 您的系統啟用單一登入（SSO）、屬於本機群組的使用者將無法登入租戶管理程式、不過他們可以根據群組權限、使用用戶端應用程式來管理租戶的資源。

2. 輸入群組名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後再編輯顯示名稱。
   - 聯盟群組：輸入唯一名稱。對於Active Directory、唯一名稱是與相關聯的名稱 `sAMAccountName` 屬性。對於OpenLDAP、唯一名稱是與相關聯的名稱 `uid` 屬性。
3. 選擇*繼續*。

管理群組權限

群組權限可控制使用者可在租戶管理器和租戶管理 API 中執行的工作。

步驟

1. 對於 * 存取模式 * 、請選取下列其中一項：
   - * 讀寫 *（預設）：使用者可以登入租戶管理員並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。他們無法在租戶管理員或租戶管理 API 中進行任何變更或執行任何作業。本機唯讀使用者可以變更自己的密碼。

     如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。

2. 如果群組使用者需要登入租戶管理員或租戶管理 API 、請選取 * 根存取 * 核取方塊。
3. 選擇*繼續*。

設定 **Swift** 群組原則

Swift 使用者需要系統管理員權限才能驗證 Swift REST API 、以建立容器和擷取物件。

1. 如果群組使用者需要使用 Swift REST API 來管理容器和物件、請選取 * Swift 管理員 * 核取方塊。
2. 如果您要建立本機群組、請選取*繼續*。如果您要建立聯盟群組、請選取*建立群組*和*完成*。

新增使用者（僅限本機群組）

您可以儲存群組而不新增使用者、也可以選擇性地新增已存在的任何本機使用者。

步驟

1. 您也可以為此群組選取一或多個本機使用者。

   如果您尚未建立本機使用者、可以在「使用者」頁面上將此群組新增至使用者。請參閱 "管理本機使用者"。

2. 選擇* Create group（創建組）和 Finish（完成）*。

   您建立的群組會出現在群組清單中。

租戶管理權限

建立租戶群組之前、請先考量您要指派給該群組的權限。租戶管理權限可決定使用者可以使用租戶管理程式或租戶管理API執行哪些工作。使用者可以屬於一或多個群組。如果使用者屬於多個群組、則權限是累積性的。

若要登入租戶管理程式或使用租戶管理API、使用者必須屬於至少擁有一項權限的群組。所有可以登入的使用者都可以執行下列工作：

- 檢視儀表板
- 變更自己的密碼（適用於本機使用者）

對於所有權限、群組的存取模式設定會決定使用者是否可以變更設定及執行作業、或是只能檢視相關設定和功能。

如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。

您可以將下列權限指派給群組。請注意、S3租戶和Swift租戶擁有不同的群組權限。

權限	說明
root存取權	提供租戶管理程式和租戶管理API的完整存取權限。 • 附註： * Swift 使用者必須擁有 root 存取權限、才能登入租戶帳戶。

權限	說明
系統管理員	僅限Swift租戶。提供此租戶帳戶的Swift容器和物件的完整存取權 附註： Swift使用者必須擁有Swift管理員權限、才能使用Swift REST API執行任何作業。
管理您自己的 S3 認證	可讓使用者建立及移除自己的S3存取金鑰。沒有此權限的使用者不會看到 * 儲存設備（ S3 ） * > * My S3 存取鍵 * 功能表選項。
管理所有貯體	• S3租戶：可讓使用者使用租戶管理程式和租戶管理API來建立及刪除S3桶、並管理租戶帳戶中所有S3桶的設定、無論S3桶或群組原則為何。 沒有此權限的使用者不會看到 * 「鏟斗」 * 功能表選項。 • Swift租戶：可讓Swift使用者使用租戶管理API來控制Swift Container的一致性層級。 • 注意： * 您只能從租戶管理 API 將「管理所有貯體」權限指派給 Swift 群組。您無法使用 Tenant Manager 將此權限指派給 Swift 群組。
管理端點	可讓使用者使用租戶管理器或租戶管理 API 來建立或編輯平台服務端點、這些端點是 StorageGRID 平台服務的目的地。 沒有此權限的使用者不會看到 * 平台服務端點 * 功能表選項。
使用 S3 主控台管理物件	結合「管理所有貯體」權限、可讓使用者從「貯體」頁面存取實驗 S3 主控台。擁有此權限但沒有「管理所有儲存區」權限的使用者仍可直接瀏覽至實驗 S3 主控台。

管理群組

您可以檢視群組、編輯群組的名稱、權限、原則和使用者、複製群組； 或刪除群組。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。

檢視或編輯群組

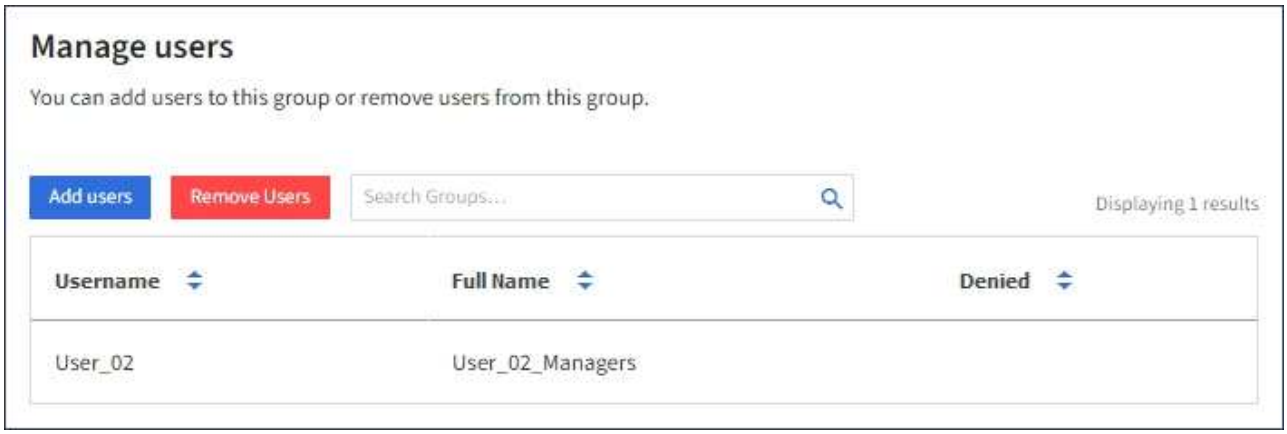
您可以檢視和編輯每個群組的基本資訊和詳細資料。

步驟

1. 選擇*存取管理*>*群組*。
2. 檢閱「群組」頁面上提供的資訊、其中列出此租戶帳戶所有本機和同盟群組的基本資訊。

   如果租戶帳戶具有 * 使用網格同盟連線 * 權限、且您正在租戶來源網格上檢視群組、則藍色橫幅會指出、如果您編輯或移除群組、您的變更將不會同步到其他網格。請參閱 "複製租戶群組和使用者"。

3. 如果您要變更群組名稱：
   a. 選取群組的核取方塊。
   b. 選擇*操作*>*編輯群組名稱*。
   c. 輸入新名稱。
   d. 選取 * 儲存變更 *
4. 如果您想要檢視更多詳細資料或進行其他編輯、請執行下列其中一項：
   - 選取群組名稱。
   - 選取群組的核取方塊、然後選取 * 動作 * > * 檢視群組詳細資料 * 。
5. 檢閱「總覽」一節、其中顯示每個群組的下列資訊：
   - 顯示名稱
   - 唯一名稱
   - 類型
   - 存取模式
   - 權限
   - S3 原則
   - 此群組中的使用者數目
   - 如果租戶帳戶具有「 * 使用網格同盟連線 * 」權限、且您正在租戶來源網格上檢視群組、則會顯示其他欄位：
     - 克隆狀態，可以是 * 成功 * 或 * 失敗 *
     - 藍色橫幅表示如果您編輯或刪除此群組、您的變更將不會同步至其他網格。
6. 視需要編輯群組設定。請參閱 "為S3租戶建立群組" 和 "為Swift租戶建立群組" 以取得有關輸入內容的詳細資訊。
   a. 在「總覽」區段中、選取名稱或編輯圖示以變更顯示名稱 。
   b. 在 * 群組權限 * 索引標籤上、更新權限、然後選取 * 儲存變更 * 。
   c. 在 * 群組原則 * 索引標籤上、進行任何變更、然後選取 * 儲存變更 * 。
      - 如果您正在編輯 S3 群組、請視需要選擇不同的 S3 群組原則、或輸入自訂原則的 JSON 字串。
      - 如果您正在編輯 Swift 群組、請選擇或清除 **Swift Administrator** 核取方塊。
7. 若要將一或多個現有的本機使用者新增至群組：
   a. 選取使用者索引標籤。



b. 選取 * 新增使用者 * 。

c. 選取您要新增的現有使用者、然後選取 * 新增使用者 * 。

右上角會出現成功訊息。

8. 若要從群組中移除本機使用者：

a. 選取使用者索引標籤。

b. 選取 * 移除使用者 * 。

c. 選取您要移除的使用者、然後選取 * 移除使用者 * 。

右上角會出現成功訊息。

9. 確認您為變更的每個區段選擇了 * 儲存變更 * 。

複製群組

您可以複製現有群組、以更快建立新群組。

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、而且您從租戶的來源網格複製群組、則複製的群組將會複製到租戶的目的地網格。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要複製之群組的核取方塊。
3. 選取*「動作*」>*「重複群組*」。
4. 請參閱 "為S3租戶建立群組" 或 "為Swift租戶建立群組" 以取得有關輸入內容的詳細資訊。
5. 選取*建立群組*。

刪除一或多個群組

您可以刪除一或多個群組。只屬於已刪除群組的任何使用者將無法再登入租戶管理員或使用租戶帳戶。

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、而且您刪除了群組、 StorageGRID 將不會刪除其他網格上的對應群組。如果您需要保持此資訊同步、您必須從兩個方格中刪除相同的群組。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要刪除的每個群組的核取方塊。
3. 選擇 * 行動 * > * 刪除群組 * 或 * 行動 * > * 刪除群組 * 。

   隨即顯示確認對話方塊。

4. 選取 * 刪除群組 * 或 * 刪除群組 * 。

管理本機使用者

您可以建立本機使用者並將其指派給本機群組、以決定這些使用者可以存取哪些功能。租戶管理程式包含一個預先定義的本機使用者、名為「 root 」。 雖然您可以新增及移除本機使用者、但無法移除根使用者。

如果您的 StorageGRID 系統啟用單一登入（ SSO ）、本機使用者將無法登入租戶管理員或租戶管理 API 、不過他們可以根據群組權限使用用戶端應用程式來存取租戶的資源。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、您已檢閱的工作流程和考量事項 "複製租戶群組和使用者"，您將登入租戶的來源網格。

建立本機使用者

您可以建立本機使用者並將其指派給一或多個本機群組、以控制其存取權限。

不屬於任何群組的 S3 使用者沒有管理權限或 S3 群組原則套用到他們。這些使用者可能會透過儲存區原則授予S3儲存區存取權。

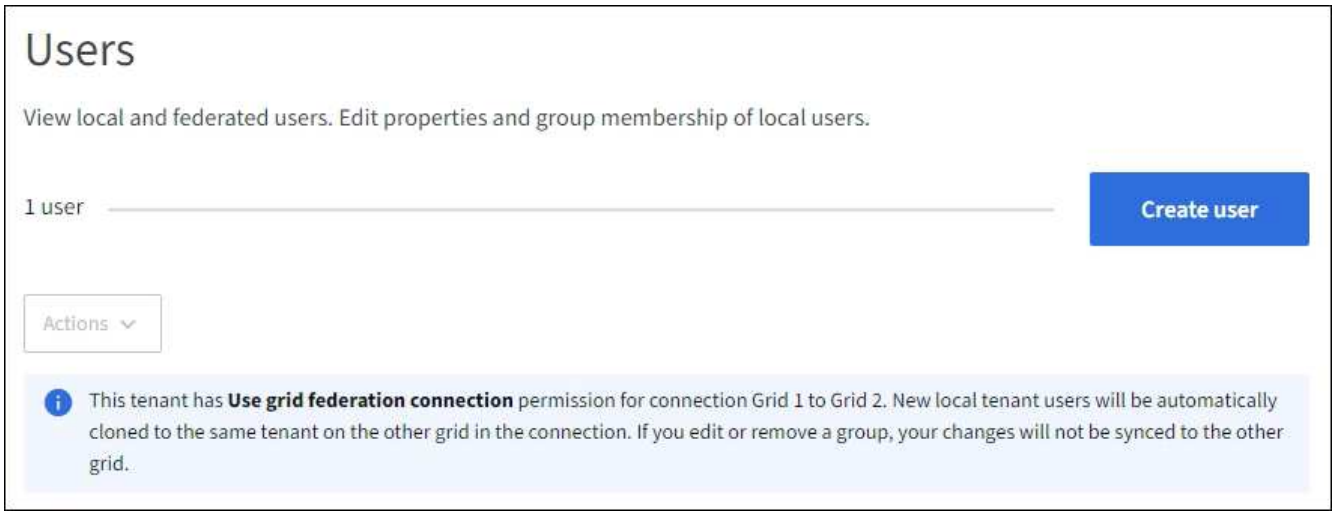
不屬於任何群組的 Swift 使用者沒有管理權限或 Swift Container 存取權。

存取建立使用者精靈

步驟

1. 選擇*存取管理*>*使用者*。

   如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則藍色橫幅會指出這是租戶的來源網格。您在此網格上建立的任何本機使用者都會複製到連線中的其他網格。



2. 選取*建立使用者*。

輸入認證

步驟

1. 對於 * 輸入使用者認證 * 步驟、請填寫下列欄位。

欄位	說明
全名	此使用者的全名、例如人員的名字和姓氏、或應用程式的名稱。
使用者名稱	此使用者將用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。 • 附註 * ：如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則如果目的地網格上的租戶已經存在相同的 * 使用者名稱 * 、就會發生複製錯誤。
密碼和確認密碼	使用者在登入時最初使用的密碼。
拒絕存取	選取 * 是 * 可防止此使用者登入租戶帳戶、即使他們仍屬於一個或多個群組。 例如、選取 * 是 * 可暫時暫停使用者登入的能力。

2. 選擇*繼續*。

指派給群組

步驟

1. 將使用者指派給一或多個本機群組、以判斷他們可以執行哪些工作。

   將使用者指派給群組是選擇性的。如果您願意、可以在建立或編輯群組時選取使用者。

   不屬於任何群組的使用者將沒有管理權限。權限是累積性的。使用者將擁有所屬所有群組的所有權限。請參閱 "租戶管理權限"。

2. 選取*建立使用者*。

   如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您位於租戶的來源網格上、則新的本機使用者會複製到租戶的目的地網格。* 成功 * 會在使用者詳細資料頁面的「概述」區段中顯示為 * 複製狀態 * 。

3. 選擇 * 完成 * 返回「使用者」頁面。

檢視或編輯本機使用者

步驟

1. 選擇*存取管理*>*使用者*。
2. 檢閱「使用者」頁面上提供的資訊、其中列出此租戶帳戶所有本機和同盟使用者的基本資訊。

   如果租戶帳戶具有 * 使用網格同盟連線 * 權限、且您正在租戶來源網格上檢視使用者、則藍色橫幅會指出、如果您編輯或移除使用者、您的變更將不會同步到其他網格。

3. 若要變更使用者的全名：
   a. 選取使用者的核取方塊。
   b. 選擇* Actions > Edit full name*（操作>*編輯全名*）。
   c. 輸入新名稱。
   d. 選取 * 儲存變更 *
4. 如果您想要檢視更多詳細資料或進行其他編輯、請執行下列其中一項：
   - 選取使用者名稱。
   - 選取使用者的核取方塊、然後選取 * 動作 * > * 檢視使用者詳細資料 * 。
5. 檢閱「總覽」一節、其中顯示每位使用者的下列資訊：
   - 全名
   - 使用者名稱
   - 使用者類型
   - 拒絕存取
   - 存取模式
   - 群組成員資格
   - 如果租戶帳戶具有「 * 使用網格同盟連線 * 」權限、且您正在租戶來源網格上檢視使用者、則會顯示其他欄位：
     - 克隆狀態，可以是 * 成功 * 或 * 失敗 *
     - 藍色橫幅表示如果您編輯此使用者、您的變更將不會同步至其他網格。
6. 視需要編輯使用者設定。請參閱 建立本機使用者 以取得有關輸入內容的詳細資訊。
   a. 在「總覽」區段中、選取名稱或編輯圖示以變更全名  。

      您無法變更使用者名稱。

   b. 在 * 密碼 * 標籤上、變更使用者的密碼、然後選取 * 儲存變更 * 。

c. 在 * 存取 * 索引標籤上、選取 * 否 * 以允許使用者登入、或選取 * 是 * 以防止使用者登入。然後選取 * 儲存變更 * 。

d. 在 * 存取金鑰 * 索引標籤上、選取 * 建立金鑰 * 、然後依照的指示進行 "建立其他使用者的 S3 存取金鑰 "。

e. 在 * 群組 * 索引標籤上、選取 * 編輯群組 * 、將使用者新增至群組或從群組中移除使用者。然後選取 * 儲存變更 * 。

7. 確認您為變更的每個區段選擇了 * 儲存變更 * 。

重複的本機使用者

您可以複製本機使用者、以更快建立新使用者。

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您從租戶的來源網格複製使用者、則複製的使用者將會複製到租戶的目的地網格。

步驟

1. 選擇*存取管理*>*使用者*。
2. 選取您要複製之使用者的核取方塊。
3. 選取*「動作*」>*「重複使用者*」。
4. 請參閱 建立本機使用者 以取得有關輸入內容的詳細資訊。
5. 選取*建立使用者*。

刪除一或多個本機使用者

您可以永久刪除不再需要存取 StorageGRID 租戶帳戶的一或多個本機使用者。

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您刪除了本機使用者、 StorageGRID 將不會刪除其他網格上的對應使用者。如果您需要保持此資訊同步、則必須從兩個方格中刪除相同的使用者。

您必須使用同盟識別來源來刪除同盟使用者。

步驟

1. 選擇*存取管理*>*使用者*。
2. 選取您要刪除的每個使用者的核取方塊。
3. 選擇 * 行動 * > * 刪除使用者 * 或 * 行動 * > * 刪除使用者 * 。

   隨即顯示確認對話方塊。

4. 選取 * 刪除使用者 * 或 * 刪除使用者 * 。