管理租戶群組

StorageGRID 11.8

NetApp
May 17, 2024

目錄

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	此原則範例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	詳細資料
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。	Swift 使用者必須具有「根目錄」存取權限、才能登入租戶帳戶。
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	Swift 使用者必須具有 Swift Administrator 權限、才能使用 Swift REST API 執行任何作業。

權限	說明	詳細資料
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。
檢視所有貯體	• S3 租戶 * ：可讓使用者檢視所有貯體和貯體組態。 • Swift 租戶 * ：允許 Swift 使用者使用租戶管理 API 來檢視所有容器和容器組態。	沒有「檢視所有貯體」或「管理所有貯體」權限的使用者、將不會看到「 *buckets 」功能表選項。 此權限已被「管理所有貯體」權限所取代。這不會影響 S3 用戶端或 S3 主控台所使用的 S3 儲存區或群組原則。 您只能從租戶管理 API 將此權限指派給 Swift 群組。您無法使用 Tenant Manager 將此權限指派給 Swift 群組。
管理所有貯體	*S3 租戶 * ：可讓使用者使用租戶管理員和租戶管理 API 來建立和刪除 S3 貯體、並管理租戶帳戶中所有 S3 貯體的設定、無論 S3 貯體或群組原則為何。 • Swift 租戶 * ：允許 Swift 使用者使用租戶管理 API 來控制 Swift 容器的一致性。	沒有「檢視所有貯體」或「管理所有貯體」權限的使用者、將不會看到「 *buckets 」功能表選項。 此權限取代「檢視所有貯體」權限。這不會影響 S3 用戶端或 S3 主控台所使用的 S3 儲存區或群組原則。 您只能從租戶管理 API 將此權限指派給 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 Console 標籤	與「檢視所有貯體」或「管理所有貯體」權限結合使用時、可讓使用者從儲存庫詳細資料頁面上的「 S3 主控台」索引標籤檢視及管理物件。	

管理群組

視需要管理租戶群組、以檢視、編輯或複製群組等項目。

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

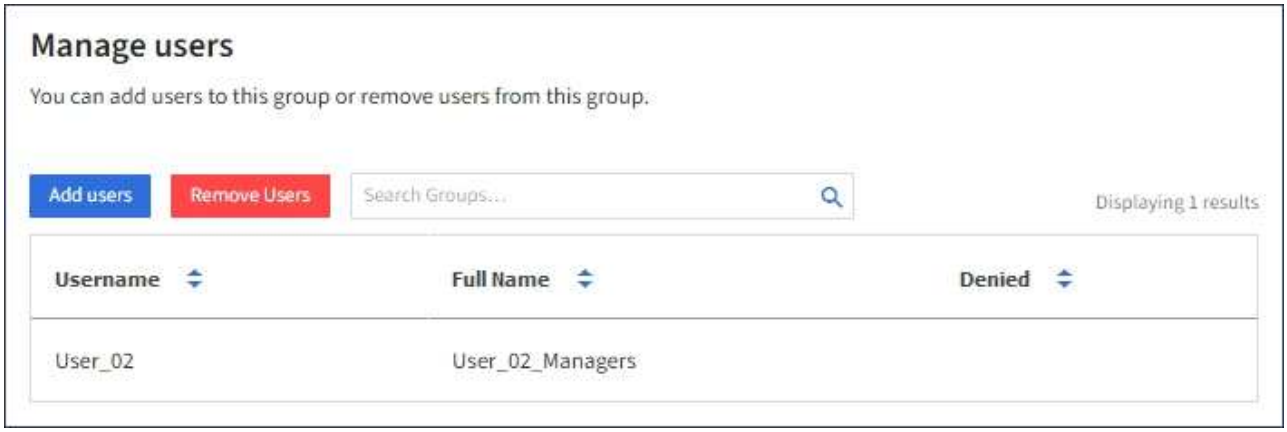
1. 選擇*存取管理*>*群組*。
2. 檢閱「群組」頁面上提供的資訊、其中列出此租戶帳戶所有本機和同盟群組的基本資訊。

   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：

   - 橫幅訊息表示如果您編輯或移除群組、您的變更將不會同步至其他網格。
   - 如有需要、橫幅訊息會指出群組是否未複製到目的地網格上的租用戶。您可以 重試群組複製 失敗了。
3. 如果您要變更群組名稱：
   a. 選取群組的核取方塊。
   b. 選取 * 動作 * > * 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*。

重試群組複製

若要重試失敗的複製：

1. 選取群組名稱下方的 _ （複製失敗） _ 的每個群組。
2. 選取 * 動作 * > * 複製群組 * 。
3. 從您要複製的每個群組的詳細資料頁面、檢視複製作業的狀態。

如需其他資訊、請參閱 "複製租戶群組和使用者"。

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 * 。