管理租戶群組

StorageGRID software

NetApp
July 23, 2026

目錄

管理租戶群組

在 StorageGRID 中為 S3 租戶建立群組

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

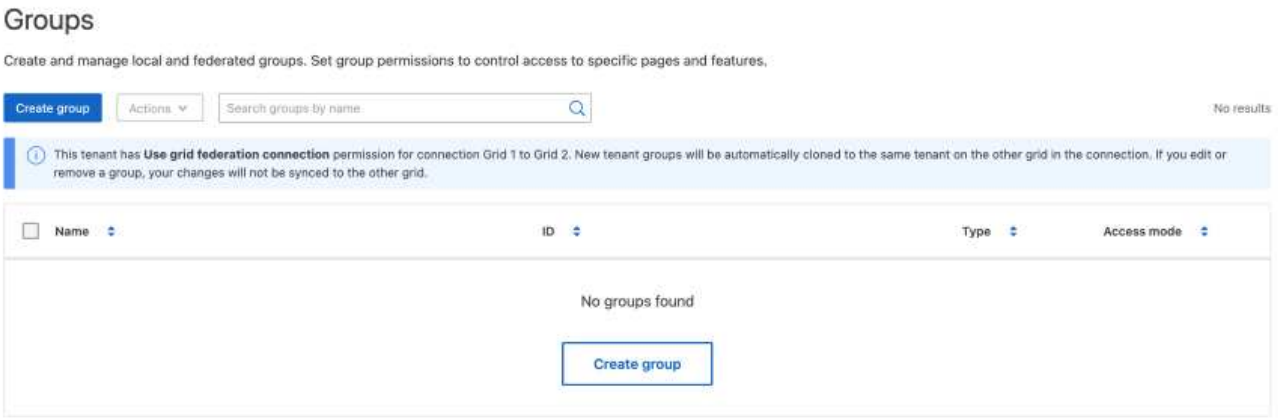
- 您已使用 "支援的網頁瀏覽器" 登入租戶管理員。
- 您屬於一個擁有 "${post_edited_translations.segment}" 的使用者群組。
- 如果您計劃匯入聯合群組，您必須已 "已設定身分識別聯盟"，且該聯合群組已存在於已設定的識別來源中。
- 如果您的租戶帳戶具有「使用網格聯合連線」權限，您已查看"Clone 租戶群組和使用者"的工作流程和注意事項，並且您已登入租戶的來源網格。

存取「建立群組精靈」

首先，存取「建立群組」精靈。

步驟

1. 選擇 **Access Management** > **Groups**。
2. 如果您的租戶帳戶擁有「使用網格聯合連線」權限，請確認是否出現藍色橫幅，該橫幅表示在此網格上建立的新群組將 Clone 到連線中另一個網格上的相同租戶。如果未出現此橫幅，則您可能已登入租戶的目的地網格。



3. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以建立本機群組或匯入聯合群組。

步驟

1. 選取「本機群組」索引標籤以建立本機群組，或選取「聯合群組」索引標籤，從先前設定的身分識別來源匯入群組。

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 Tenant Manager，但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. 請輸入群組名稱。
   - 本機群組：請同時輸入顯示名稱和唯一名稱。您可以稍後編輯顯示名稱。

     如果您的租戶帳戶具有「使用 grid federation 連線」權限，則當目的地網格上已存在與租戶相同的「唯一名稱」時，將發生 Clone 錯誤。

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

${post_edited_translations.segment}

群組權限控制使用者在租戶管理員和租戶管理 API 中可以執行哪些工作。

步驟

1. 對於 存取模式，請選擇下列其中一項：
   - 讀寫（預設）：使用者可以登入 Tenant Manager 並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。無法在 Tenant Manager 或 Tenant Management API 中進行任何變更或執行任何操作。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，且其中任何一個群組設定為唯讀，則該使用者對所有選定的設定和功能將具有唯讀存取權限。

2. 請為此群組選擇一項或多項權限。

   請參閱 "租戶管理權限"。

3. 選擇 **Continue** 。

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. 請選擇您要用於此群組的原則。

群組原則	說明
無 S3 存取權限	預設設定。此群組中的使用者無權存取 S3 資源，除非透過儲存桶原則授予存取權限。如果選擇此選項，則預設只有 root 使用者有權存取 S3 資源。

群組原則	說明
唯讀存取	此群組中的使用者對 S3 資源擁有唯讀存取。例如，此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標籤。選擇此選項後，唯讀群組原則的 JSON 字串將顯示在文字方塊中。您無法編輯此字串。
完全存取權限	此群組中的使用者擁有對 S3 資源（包括儲存桶）的完全存取權限。選擇此選項後，文字方塊中將顯示完全存取群組原則的 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儲存桶。此群組中的使用者可以執行常見操作，但無法永久刪除已啟用物件版本控制的儲存桶中的物件。 擁有 **Manage all buckets** 權限的 Tenant Manager 使用者可以置換此群組原則。請將 Manage all buckets 權限限制為受信任的使用者，並在可用時使用多因素驗證 (MFA)。
自訂	群組內使用者將獲得您在文字方塊中指定的權限。

2. 如果您選擇 **Custom**，請輸入群組原則。每個群組原則的大小限制為 5,120 位元組。您必須輸入有效的 JSON 格式字串。

   有關群組原則的詳細資訊，包括語言語法和範例，請參閱"範例群組原則"。

3. 如果要建立本機群組，請選擇「繼續」。如果要建立聯合群組，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使用者，或者您可以選擇新增任何已存在的本機使用者。

> 如果您的租戶帳戶擁有「使用網格聯合連線」權限，則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含在複製到目的地網格的群組中。因此，在建立群組時請勿選擇使用者。而應在建立使用者時選擇群組。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   您建立的群組會出現在群組清單中。

   如果您的租戶帳戶擁有 **Use grid federation connection** 權限，且您位於租戶的來源網格上，則新群組將複製到租戶的目的地網格。**Success** 會顯示為群組詳細資料頁面「概覽」區段中的 **Cloning status**。

StorageGRID 租戶管理權限

在建立租戶群組之前，請考慮要為該群組指派哪些權限。租戶管理權限決定了使用者可以使用 Tenant Manager 或 Tenant Management 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，則權限是累加的。

若要登入 Tenant Manager 或使用 Tenant Management 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以下操作：

- 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 Access mode 設定決定使用者是否可以變更設定和執行操作，或者他們是否只能檢視相關的設定和功能。

> 如果使用者屬於多個群組，且其中任何一個群組設定為唯讀，則該使用者對所有選定的設定和功能將具有唯讀存取權限。

您可以將以下權限指派給一個群組。

權限	說明	詳細資料
Root 存取	提供對租戶管理器和租戶管理 API 的完整存取權限。	
管理您自己的 S3 憑證	允許使用者建立和移除自己的 S3 存取金鑰。	沒有此權限的使用者看不到「**STORAGE (S3) > My S3 access keys**」選單選項。
檢視所有儲存桶	允許使用者檢視所有儲存桶和儲存桶組態。	沒有「View all buckets」或「Manage all buckets」權限的使用者看不到 **Buckets** 選單選項。 此權限已被「Manage all buckets」權限取代。它不會影響 S3 用戶端或 S3 Console 使用的 S3 儲存桶或群組原則。
管理所有儲存桶	允許使用者使用 Tenant Manager 和 Tenant Management API 來建立和刪除 S3 儲存桶，並管理租戶帳戶中所有 S3 儲存桶的設定，而無需考慮 S3 儲存桶或群組原則。	沒有「View all buckets」或「Manage all buckets」權限的使用者看不到 **Buckets** 選單選項。 此權限會覆寫「檢視所有儲存桶」權限。它不會影響 S3 用戶端或 S3 Console 使用的 S3 儲存桶或群組原則。
管理端點	允許使用者使用 Tenant Manager 或租戶管理 API 建立或編輯平台服務端點，這些端點用作 StorageGRID 平台服務的目的地。	沒有此權限的使用者看不到 **Platform services endpoints** 選單選項。
使用 S3 Console 索引標籤	與「View all buckets」或「Manage all buckets」權限結合使用時，允許使用者從儲存桶詳細資料頁面上的 S3 Console 索引標籤檢視和管理物件。	

管理 StorageGRID 租戶群組

根據需要管理租戶群組，以檢視、編輯或複製群組等等。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入租戶管理員。
- 您屬於一個擁有 "${post_edited_translations.segment}" 的使用者群組。

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訊。

步驟

1. 選擇 **Access Management** > **Groups**。
2. 檢視「群組」頁面上提供的資訊，其中列出此租戶帳戶所有本機群組和聯合群組的基本資訊。

   如果租戶帳戶具有「使用網格聯合連線」權限，且您正在檢視租戶來源網格上的群組：

   - 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到另一個網格。
   - 如有需要，橫幅訊息會指示群組是否未 Clone 到目的地網格上的租戶。您可以重試群組 Clone查看失敗情況。
3. 如果您想要變更群組名稱：
   a. ${post_edited_translations.segment}
   b. 選擇 **Actions** > **Edit group name**。
   c. 請輸入新名稱。
   d. 選取 儲存變更。
4. 如果想檢視更多詳細資訊或進行其他編輯，請執行以下操作之一：
   - 選取群組名稱。
   - 選取該群組的核取方塊，然後選取 **Actions** > **View group details**。
5. 請查看「概述」區段，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
   - 該群組中的使用者數量
   - 如果租戶帳戶具有「使用網格聯合連線」權限，且您正在租戶的來源網格上檢視群組，則也會顯示其他欄位：
     - Clone 狀態，為 **Success** 或 **Failure**

- 藍色橫幅提示：如果您編輯或刪除此群組，您的變更將不會同步到另一個網格。

6. 根據需要編輯群組設定。有關輸入內容的詳細資訊，請參閱 "為 S3 租戶建立群組"。
   a. 在「概覽」部分，選擇名稱或編輯圖示 即可變更顯示名稱。
   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」索引標籤上，進行任何變更，然後選取「儲存變更」。

      您也可以選擇其他 S3 群組原則，或根據需要輸入自訂原則的 JSON 字串。

7. 若要將一個或多個現有本機使用者新增至該群組：
   a. 選取「使用者」索引標籤。

   b. 選擇 **Add users**。
   c. 選擇要新增的現有使用者，然後選擇 **Add users**。

      右上角會顯示成功訊息。

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. 選擇要移除的使用者，然後選擇 **Remove users**。

      右上角會顯示成功訊息。

9. 請確認您已為修改的每個部分選擇「儲存變更」。

複製群組

您可以複製現有群組，以便更快建立新群組。

> 如果您的租戶帳戶具有「使用網格聯合連線」權限，並且您從租戶的來源網格複製一個群組，則複製的群組將會 Clone 到租戶的目的地網格。

步驟

1. 選擇 **Access Management** > **Groups**。
2. 選取要複製的群組的核取方塊。
3. ${post_edited_translations.segment}

4. 請參閱 "為 S3 租戶建立群組" 以取得輸入內容的詳細資訊。
5. ${post_edited_translations.segment}

重試群組 Clone

要重試失敗的 Clone：

1. 選擇群組名稱下方標示「（Clone 失敗）」的每個群組。
2. 選取 **Actions** > **Clone groups**。
3. 從您要 Clone 的每個群組的詳細資訊頁面檢視 Clone 作業的狀態。

如需更多資訊，請參閱"Clone 租戶群組和使用者"。

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無法再登入 Tenant Manager 或使用租戶帳戶。

> 如果您的租戶帳戶擁有 **Use grid federation connection** 權限，且您刪除了一個群組，StorageGRID 不會刪除另一個網格上的對應群組。如果您需要保持此資訊同步，則必須從兩個網格中刪除同一個群組。

步驟

1. 選擇 **Access Management** > **Groups**。
2. 選取要刪除的每個群組的核取方塊。
3. 選取 **Actions** > **Delete group** 或 **Actions** > **Delete groups**。

   ${post_edited_translations.segment}

4. 選擇*刪除群組*或*刪除群組*。

設定 AssumeRole

開始之前

您必須是系統管理員才能設定 AssumeRole。

關於此任務

若要設定 AssumeRole，請先建立要接手的目標群組（如果該群組尚不存在）。編輯該群組的 S3 原則，以指定接管該群組所允許的動作。編輯該群組的 S3 信任原則，以指定允許使用 AssumeRole API 接管該群組的受信任使用者。

透過假設此群組所建立的臨時安全性憑證有效期限有限。工作階段介於 15 分鐘到 12 小時之間，預設工作階段長為 1 小時。當您將使用者從該群組的 S3 信任原則中移除時，該使用者將無法再假設此群組。

步驟

1. 選擇 **Access Management** > **Groups**。
2. 點選群組名稱。

3. 選擇 **S3 trust policy** 索引標籤。
4. 新增您的 S3 信任原則，包括可以執行 AssumeRole 的使用者清單。
5. 選擇 **Save changes** 。
6. 選擇「S3 群組原則」索引標籤。
7. 編輯 S3 原則，僅指定此群組 S3 信任原則中新增的受信任使用者所需的 S3 動作。
8. 選擇 **Save changes** 。

AssumeRole S3 信任原則範例

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

組態完成後，S3 信任原則中列出的使用者可以執行 AssumeRole 並接收憑證。最終權限由群組原則、儲存桶原則和工作階段原則決定。如需更多資訊，請參閱 "使用存取原則"。

版權資訊

商標資訊