管理群組
StorageGRID 11.5

NetApp
April 11, 2024

目錄

管理群組

您可以指派權限給使用者群組、以控制租戶使用者可以執行的工作。您可以從身分識別來源（例如Active Directory或OpenLDAP）匯入聯盟群組、也可以建立本機群組。

如果StorageGRID 您的系統啟用單一登入（SSO）、則本機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來存取S3和Swift資源。

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。由於快取、變更可能需要15分鐘才能生效。

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。
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	僅限S3租戶。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）*>*我的S3存取金鑰*功能表選項。

權限	說明
管理所有的儲存區	• 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將不會看到「桶」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。 *附註：*您只能從租戶管理API將「管理所有桶」權限指派給Swift群組。您無法使用租戶管理程式將此權限指派給Swift群組。
管理端點	僅限S3租戶。可讓使用者使用租戶管理程式或租戶管理API來建立或編輯端點、這些端點是StorageGRID 用作支援不整平台服務的目的地。 沒有此權限的使用者不會看到*平台服務端點*功能表選項。

相關資訊

"使用S3"

"使用Swift"

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。
- 如果您打算匯入聯盟群組、表示您已設定身分識別聯盟、而且聯盟群組已存在於設定的身分識別來源中。

步驟

1. 選擇*存取管理*>*群組*。

2. 選取*建立群組*。
3. 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。

4. 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。
5. 選擇*繼續*。
6. 選取存取模式。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。
   - 讀寫（預設）：使用者可以登入租戶管理程式、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程式或租戶管理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。
7. 選取此群組的群組權限。

   請參閱租戶管理權限的相關資訊。

8. 選擇*繼續*。
9. 選取群組原則、以判斷此群組成員將擁有哪些S3存取權限。
   - 無**S3**存取：預設。此群組中的使用者沒有S3資源的存取權、除非使用資源桶原則授予存取權。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。

- 完整存取：此群組中的使用者可完整存取S3資源、包括儲存區。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。
- 自訂：群組中的使用者會被授予您在文字方塊中指定的權限。如需群組原則的詳細資訊、包括語言語法和範例、請參閱實作S3用戶端應用程式的指示。

10. 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。

    在此範例中、群組成員只能列出及存取符合其使用者名稱（金鑰前置碼）的資料夾、並在指定的儲存區中使用。請注意、在決定這些資料夾的隱私權時、應考慮其他群組原則和儲存區原則的存取權限。

11. 根據您要建立同盟群組或本機群組、選取出現的按鈕：

    - 聯盟群組：建立群組
    - 本機群組：繼續

    如果您要建立本機群組、在您選取*繼續*之後、會出現步驟4（新增使用者）。聯盟群組不會顯示此步驟。

12. 選取您要新增至群組的每個使用者核取方塊、然後選取*建立群組*。

    您也可以選擇儲存群組、而不新增使用者。您可以稍後新增使用者至群組、或在新增使用者時選取群組。

13. 選擇*完成*。

    您建立的群組會出現在群組清單中。由於快取、變更可能需要15分鐘才能生效。

相關資訊

"租戶管理權限"

"使用S3"

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。
- 如果您打算匯入聯盟群組、表示您已設定身分識別聯盟、而且聯盟群組已存在於設定的身分識別來源中。

步驟

1. 選擇*存取管理*>*群組*。

2. 選取*建立群組*。
3. 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。

4. 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。

5. 選擇*繼續*。
6. 選取存取模式。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。
   - 讀寫（預設）：使用者可以登入租戶管理程式、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程式或租戶管理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。
7. 設定群組權限。
   - 如果使用者需要登入租戶管理程式或租戶管理API、請選取*根存取*核取方塊。（預設）
   - 如果使用者不需要存取租戶管理程式或租戶管理API、請取消選取「根存取」核取方塊。例如、取消選取不需要存取租戶的應用程式核取方塊。然後、指派* Swift管理員*權限、讓這些使用者能夠管理容器和物件。
8. 選擇*繼續*。
9. 如果使用者需要使用Swift REST API、請選取「* Swift管理員*」核取方塊。

   Swift使用者必須擁有root存取權限、才能存取租戶管理程式。不過、「根存取」權限不允許使用者驗證Swift REST API、以建立容器和擷取物件。使用者必須具有Swift Administrator權限、才能驗證到Swift REST API。
10. 根據您要建立同盟群組或本機群組、選取出現的按鈕：
    - 聯盟群組：建立群組
    - 本機群組：繼續

      如果您要建立本機群組、在您選取*繼續*之後、會出現步驟4（新增使用者）。聯盟群組不會顯示此步驟。
11. 選取您要新增至群組的每個使用者核取方塊、然後選取*建立群組*。

    您也可以選擇儲存群組、而不新增使用者。您可以稍後新增使用者至群組、或在建立新使用者時選取群組。
12. 選擇*完成*。

    您建立的群組會出現在群組清單中。由於快取、變更可能需要15分鐘才能生效。

相關資訊

"租戶管理權限"

"使用Swift"

檢視及編輯群組詳細資料

當您檢視群組的詳細資料時、可以變更群組的顯示名稱、權限、原則及屬於群組的使用者。

您需要的產品

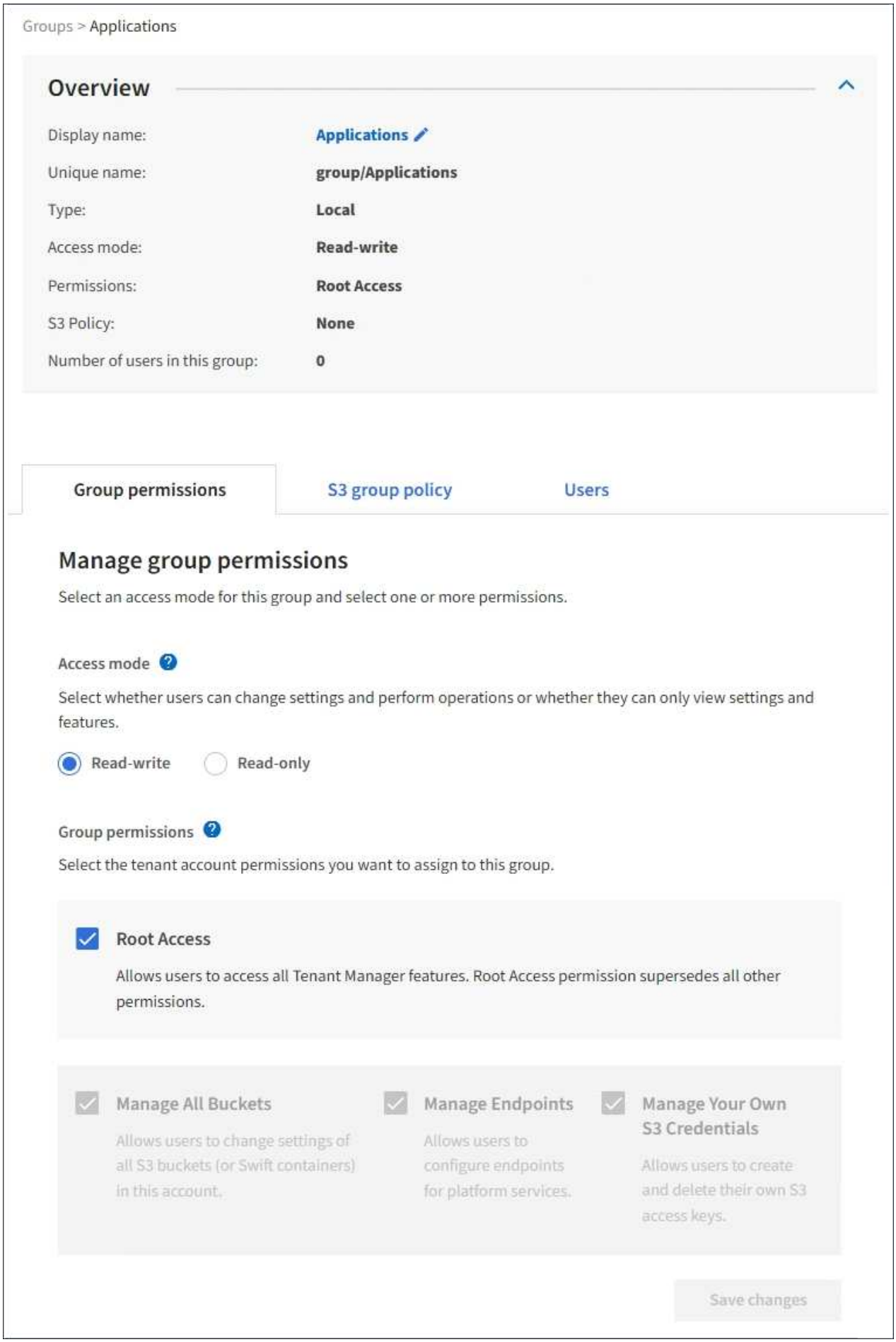
- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要檢視或編輯其詳細資料的群組名稱。

   或者、您也可以選取*「動作」>「檢視群組詳細資料」*。

   隨即顯示群組詳細資料頁面。以下範例顯示S3群組詳細資料頁面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 視需要變更群組設定。

   若要確保儲存變更、請在每個區段進行變更後、選取*儲存變更*。儲存變更時、頁面右上角會出現確認訊息。

   a. 或者、選取顯示名稱或編輯圖示 以更新顯示名稱。

      您無法變更群組的唯一名稱。您無法編輯同盟群組的顯示名稱。

   b. 或者、請更新權限。

   c. 針對群組原則、請針對S3或Swift租戶進行適當的變更。

      - 如果您正在編輯S3租戶的群組、請選擇不同的S3群組原則。如果您選取自訂S3原則、請視需要更新Json字串。
      - 如果您正在編輯Swift租戶的群組、請選擇或取消選取「* Swift管理員*」核取方塊。

        如需Swift Administrator權限的詳細資訊、請參閱建立Swift租戶群組的指示。

   d. 或者、新增或移除使用者。

4. 確認您已針對每個變更的區段選擇*儲存變更*。

   由於快取、變更可能需要15分鐘才能生效。

相關資訊

"為S3租戶建立群組"

"為Swift租戶建立群組"

新增使用者至本機群組

您可以視需要將使用者新增至本機群組。

您需要的產品

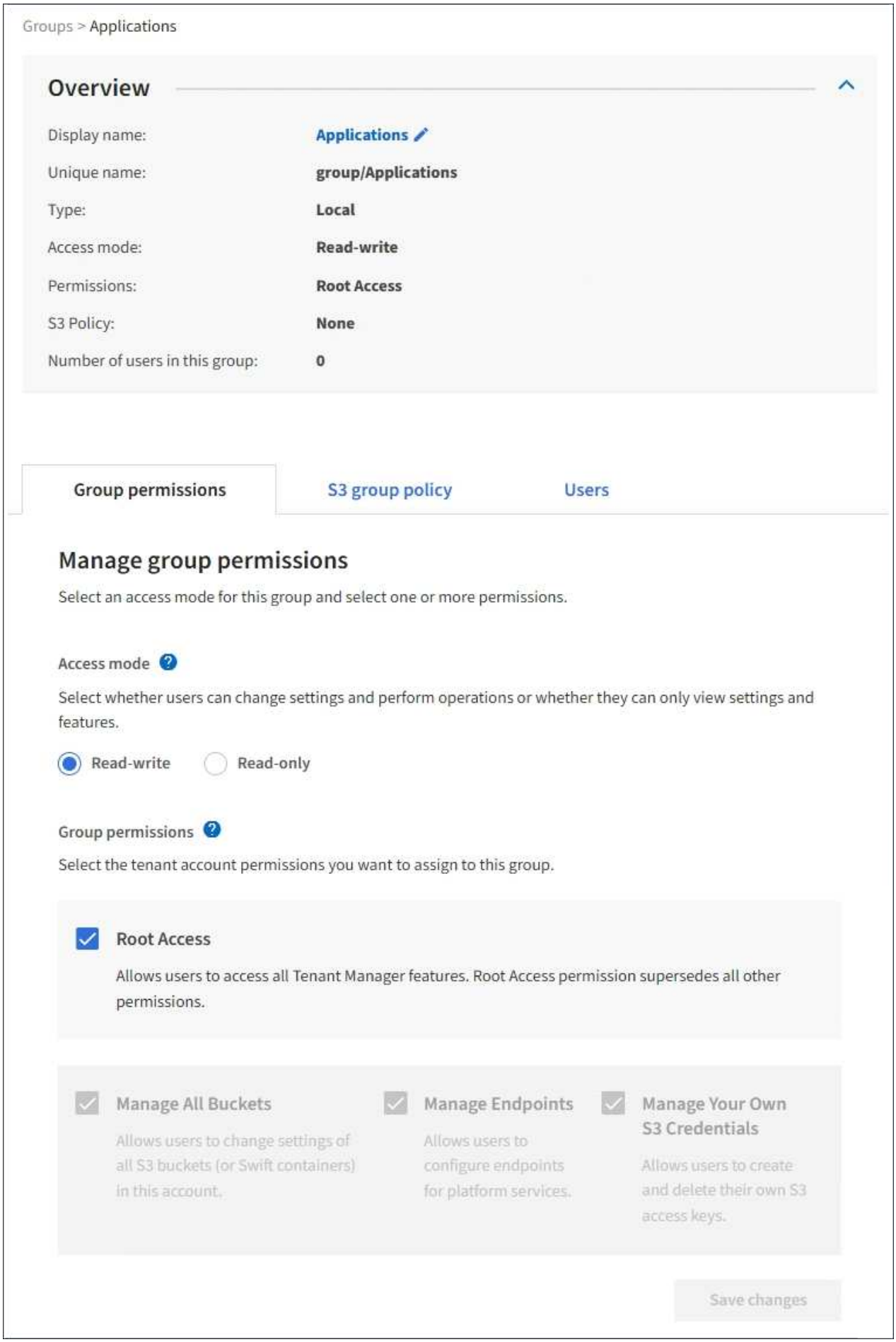
- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

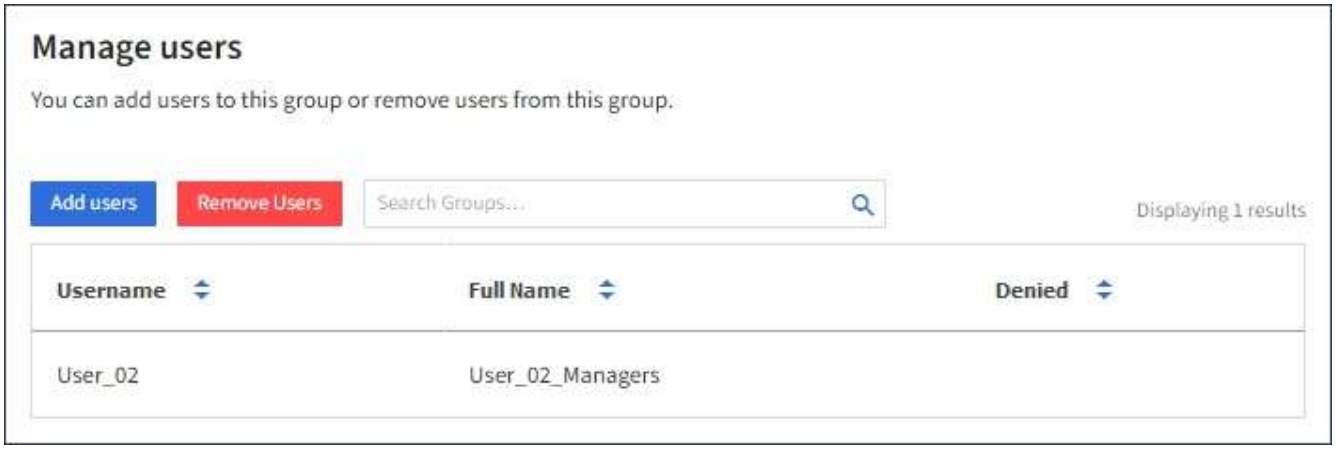
1. 選擇*存取管理*>*群組*。
2. 選取您要新增使用者的本機群組名稱。

   或者、您也可以選取*「動作」>「檢視群組詳細資料」*。

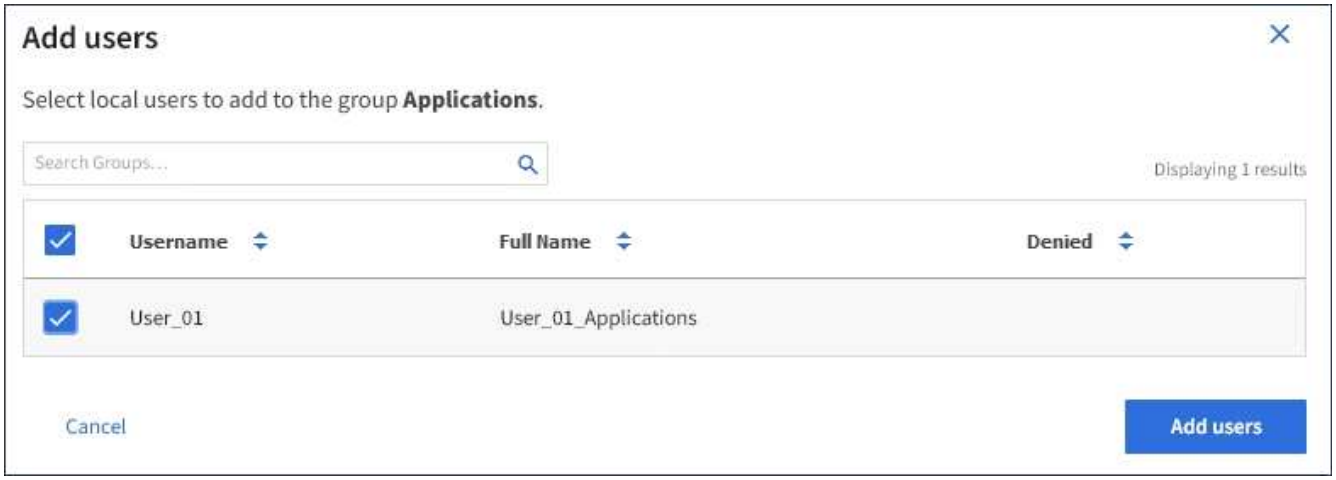
   隨即顯示群組詳細資料頁面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 選取*管理使用者*、然後選取*新增使用者*。



4. 選取您要新增至群組的使用者、然後選取*新增使用者*。



頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

編輯群組名稱

您可以編輯群組的顯示名稱。您無法編輯群組的唯一名稱。

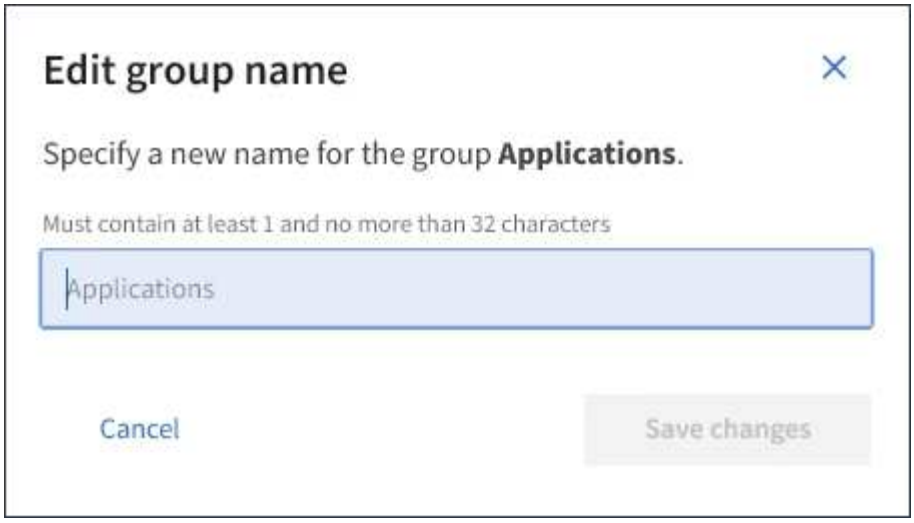
您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要編輯其顯示名稱之群組的核取方塊。
3. 選擇*操作*>*編輯群組名稱*。

「編輯群組名稱」對話方塊隨即出現。



4. 如果您正在編輯本機群組、請視需要更新顯示名稱。

   您無法變更群組的唯一名稱。您無法編輯同盟群組的顯示名稱。

5. 選取*儲存變更*。

   頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

相關資訊

"租戶管理權限"

複製群組

您可以複製現有群組、以更快建立新群組。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

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. 選擇*複製群組*。如需建立群組的其他詳細資料、請參閱建立S3租戶或Swift租戶群組的指示。
4. 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。

5. 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。

6. 選擇*繼續*。
7. 視需要修改此群組的權限。
8. 選擇*繼續*。
9. 如有需要、如果您要複製S3租戶的群組、請從*新增S3原則*選項按鈕中選擇不同的原則。如果您選取自訂原則、請視需要更新Json字串。
10. 選取*建立群組*。

相關資訊

"為S3租戶建立群組"

"為Swift租戶建立群組"

"租戶管理權限"

刪除群組

您可以從系統中刪除群組。只屬於該群組的任何使用者將無法再登入租戶管理程式或使用租戶帳戶。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

1. 選擇*存取管理*>*群組*。

2. 選取您要刪除之群組的核取方塊。
3. 選擇*操作*>*刪除群組*。

   隨即顯示確認訊息。

4. 選擇*刪除群組*以確認您要刪除確認訊息中所示的群組。

   頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

相關資訊

"租戶管理權限"

版權資訊

商標資訊