管理系統存取
StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-116/tenant/using-identity-federation.html on October 03, 2025. Always check docs.netapp.com for the latest.

目錄

管理系統存取

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。

您需要的產品

- 您將使用登入租戶管理程式 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 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

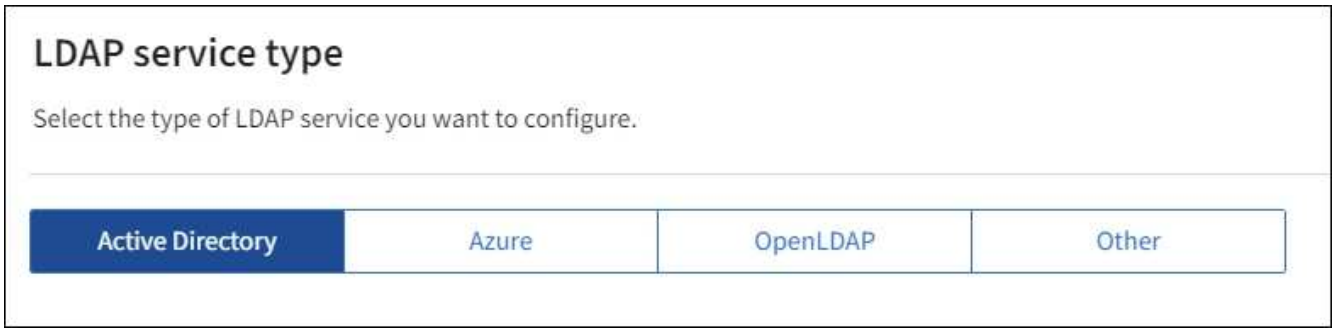
您是否可以為租戶設定身分識別聯盟服務、取決於租戶帳戶的設定方式。您的租戶可能會共用為Grid Manager設定的身分識別聯盟服務。如果您在存取「身分識別聯盟」頁面時看到此訊息、則無法為此租戶設定個別的聯盟身分識別來源。

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.

輸入組態

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Active Directory的「shamAccountName」和OpenLDAP的「uid」。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Active Directory的「objectGuid」和OpenLDAP的「entryUUID」。如果要配置Oracle Directory Server、請輸入「nssiuniuniid」。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Active Directory的「shamAccountName」和OpenLDAP的「CN」。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Active Directory的「objectGuid」和OpenLDAP的「entryUUID」。如果要配置Oracle Directory Server、請輸入「nssiuniuniid」。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：

     - 「AMAccountName」或「uid」
     - "objectGUID"、"entryUUUID"或"nssiuniuniid"
     - 《中國》
     - 「memberof」或「isMemberOf」
     - * Active Directory *：「objectSid」、「primaryGroupID」、「userAccountControl」及「userPrincipalName」

- * Azure *：「帳戶已啟用」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StorageGRID 無法自動判斷模式、則應使用預設的使用者名稱模式。

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：

- 使用者主體名稱模式（**Active Directory**和**Azure**）：「[username]@*example*.com」
- 低層級登入名稱模式（**Active Directory**和**Azure**）：「*example*\[username]」
- 辨別名稱模式：「CN=[username]、CN=Users、DC=*examends*、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。

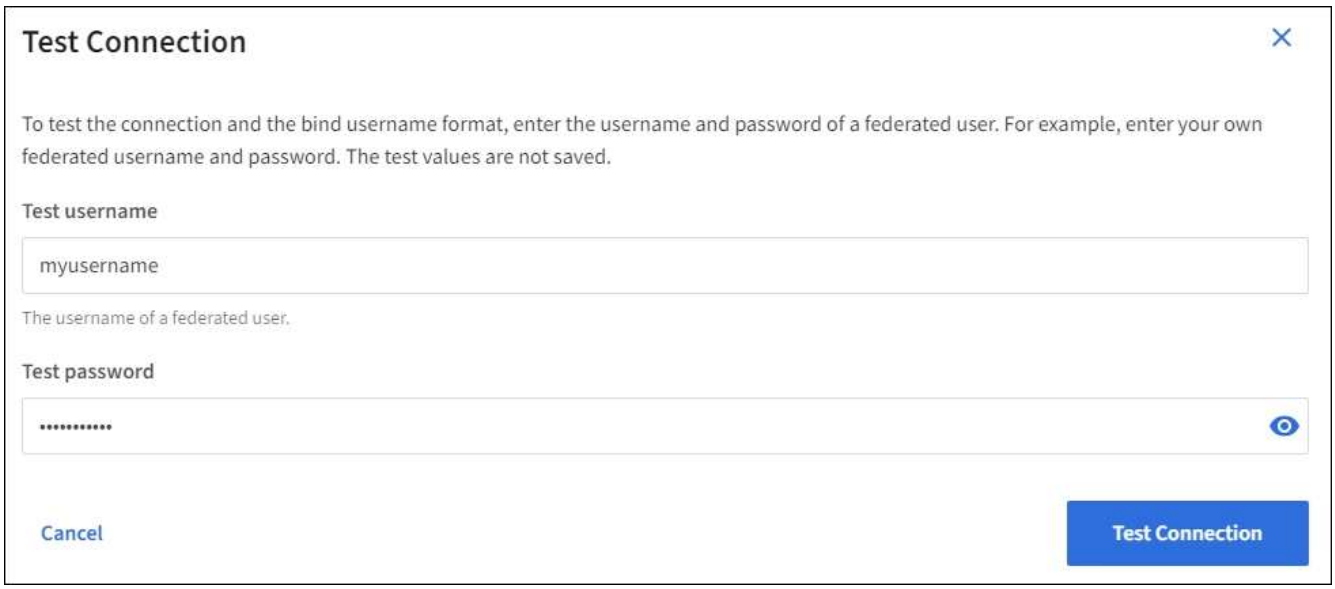
如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

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

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。
- 如果單一登入（SSO）設定為*已啟用*或*沙箱模式*、則「啟用身分聯盟」核取方塊會停用。「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. 取消核取「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 無法自動封鎖S3存取外部停用的使用者。若要封鎖S3存取、請刪除使用者的任何S3金鑰、並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。

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。請參閱 租戶管理權限。
- 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。

如需S3的相關資訊、請參閱 使用S3。

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「shamAccountName」屬性相關聯的名稱。對於OpenLDAP、唯一名稱是與「uid」屬性相關聯的名稱。
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。

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

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 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「shamAccountName」屬性相關聯的名稱。對於OpenLDAP、唯一名稱是與「uid」屬性相關聯的名稱。
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

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。
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

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

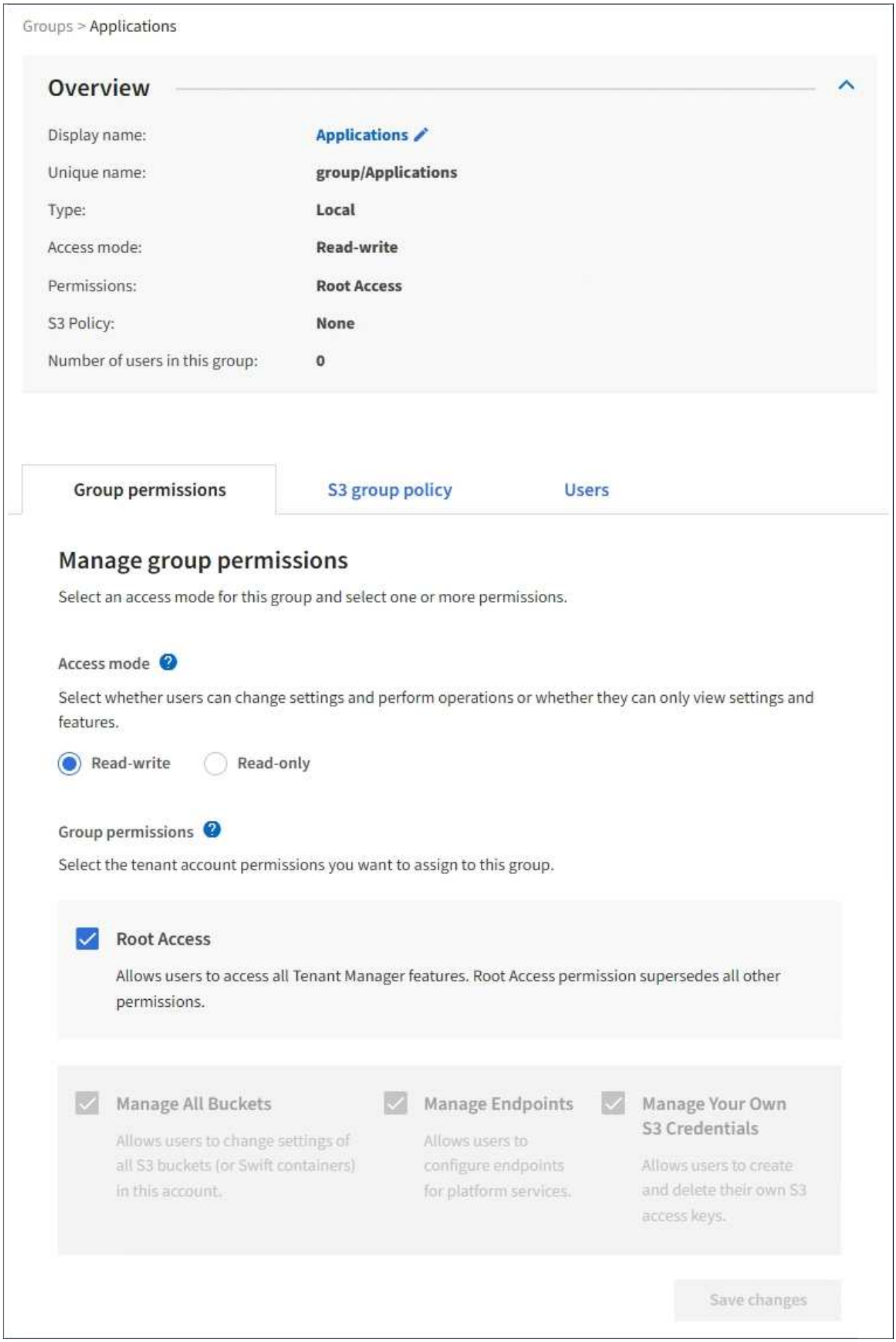
- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。

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

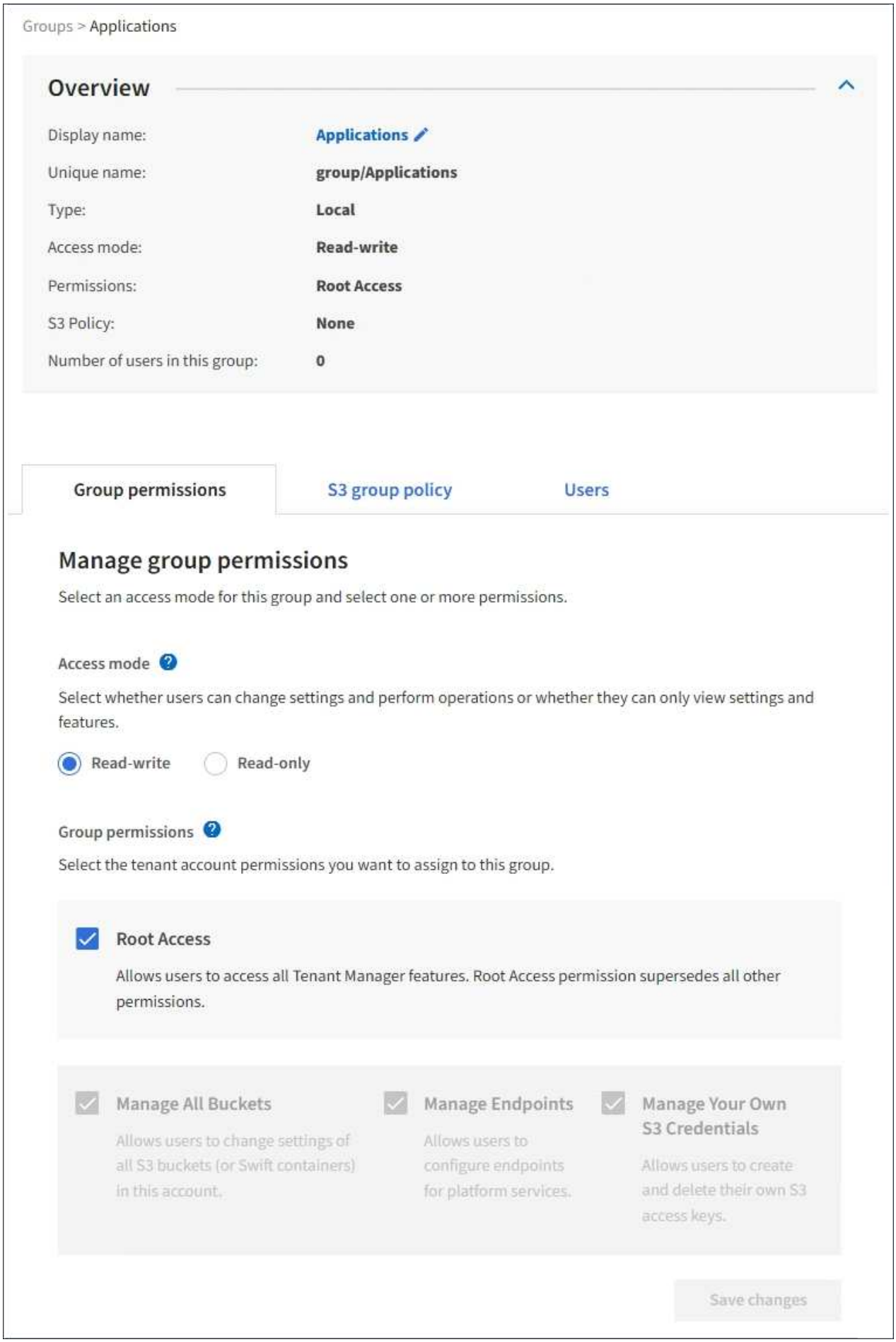
- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

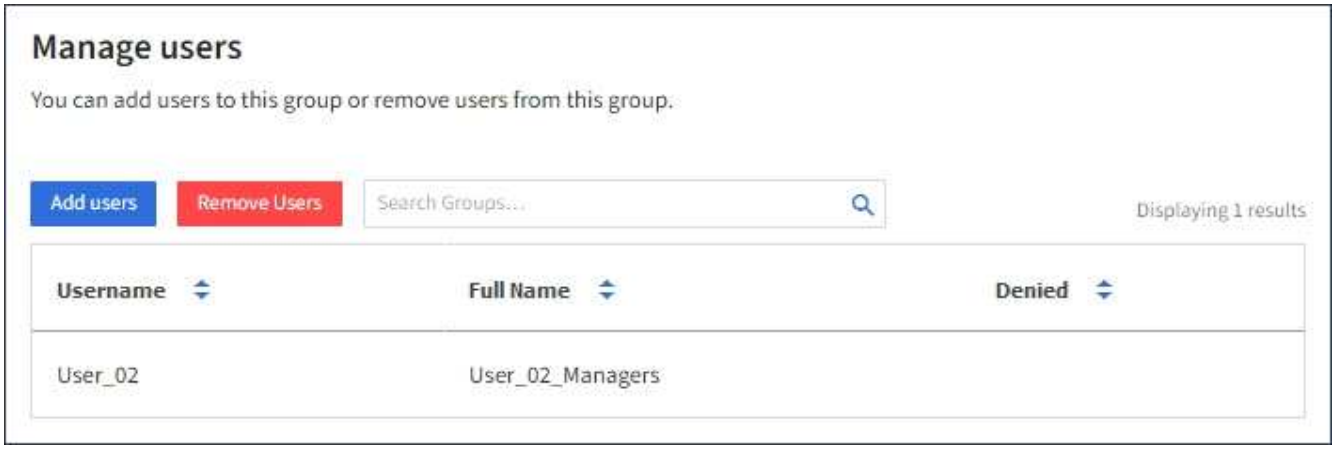
1. 選擇*存取管理*>*群組*。
2. 選取您要新增使用者的本機群組名稱。

   或者、您也可以選取*「動作」>「檢視群組詳細資料」*。

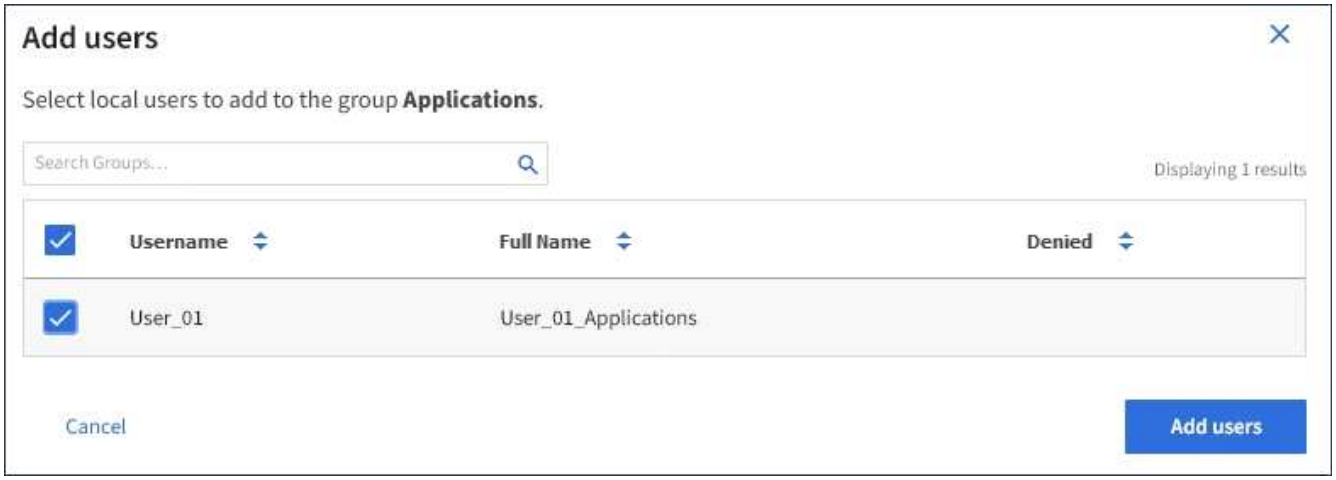
   隨即顯示群組詳細資料頁面。


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*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。

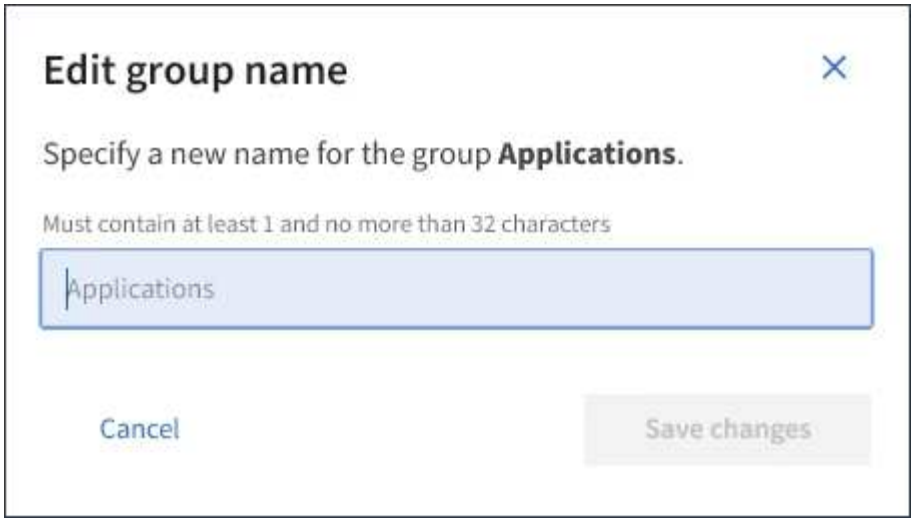
您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。請參閱 租戶管理權限。

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。

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

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。請參閱 租戶管理權限。

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、請參閱建立群組的指示 S3租戶 或是 Swift租戶。
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 您的支援系統啟用單一登入（SSO）、屬於本機群組的使用者將無法登入租戶管理程式、不過他們可以使用用戶端應用程式來管理租戶的資源、 根據群組權限。

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「shamAccountName」屬性相關聯的名稱。對於OpenLDAP、唯一名稱是與「uid」屬性相關聯的名稱。
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*。

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

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。請參閱 租戶管理權限。

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。

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root使用者。

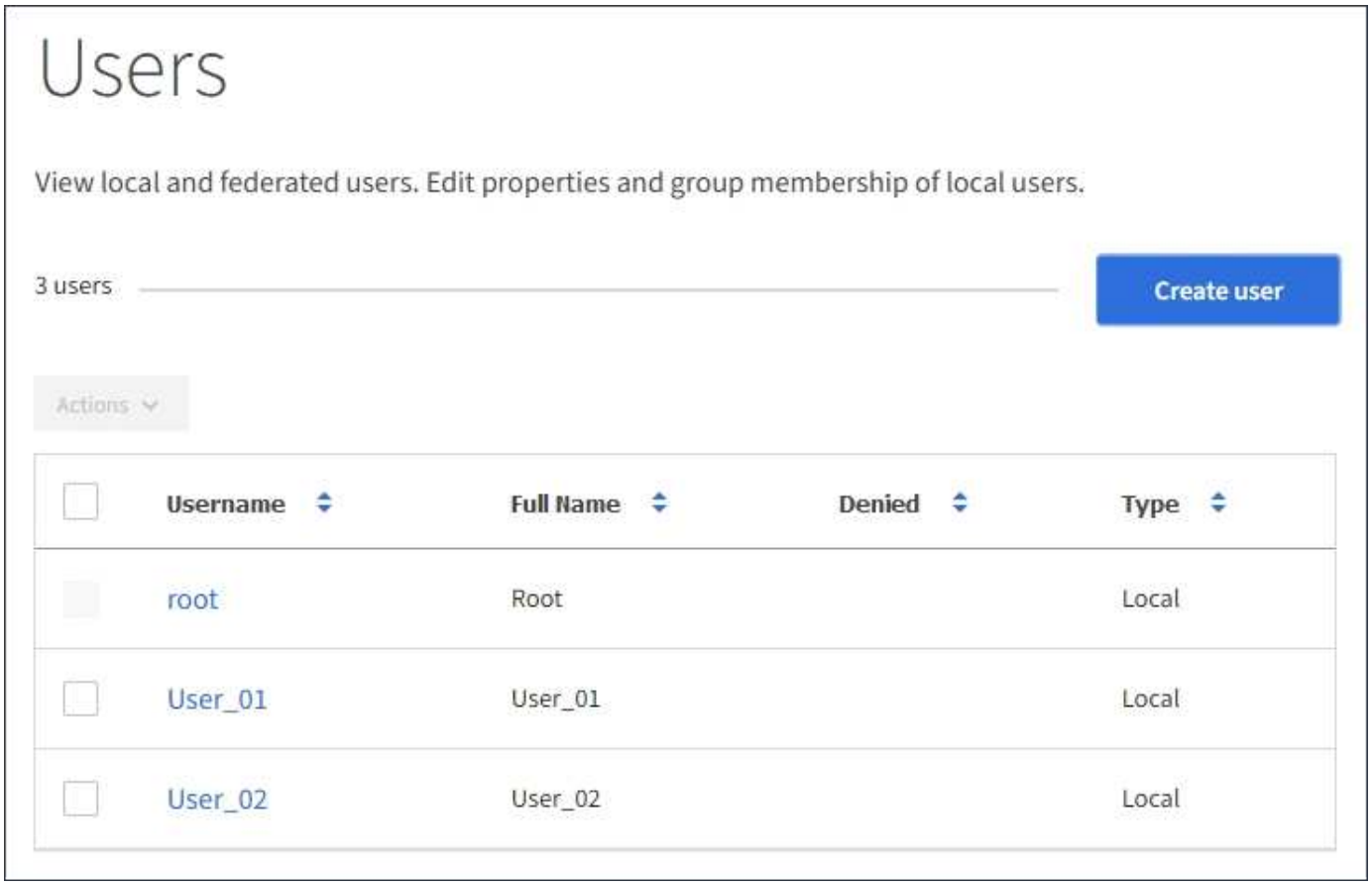
您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的讀寫使用者群組。請參閱 租戶管理權限。

> 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或租戶管理API、不過他們可以根據群組權限、使用S3或Swift用戶端應用程式來存取租戶的資源。

存取「使用者」頁面

選擇*存取管理*>*使用者*。



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使用者沒有套用管理權限或S3群組原則。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使用者不具備管理權限或Swift Container存取權。

步驟

1. 選取*建立使用者*。
2. 填寫下列欄位。
   - 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：此使用者用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。
   - 密碼：使用者登入時使用的密碼。
   - 確認密碼：在「密碼」欄位中輸入相同的密碼。
   - 拒絕存取：如果您選取*是*、此使用者就無法登入租戶帳戶、即使該使用者仍屬於一或多個群組。

     例如、您可以使用此功能暫時暫停使用者登入的能力。
3. 選擇*繼續*。
4. 將使用者指派給一或多個本機群組。

   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。
5. 選取*建立使用者*。

   由於快取、變更可能需要15分鐘才能生效。

編輯使用者詳細資料

當您編輯使用者的詳細資料時、可以變更使用者的全名和密碼、將使用者新增至不同的群組、以及防止使用者存取租戶。

步驟

1. 在使用者清單中、選取您要檢視或編輯其詳細資料的使用者名稱。

   或者、您也可以選取使用者的核取方塊、然後選取*「Actions」（動作）>「View user details」（檢視使用者詳細資料）*。
2. 視需要變更使用者設定。
   a. 選取全名或編輯圖示、視需要變更使用者的全名 在「總覽」區段中。

      您無法變更使用者名稱。
   b. 在*密碼*索引標籤上、視需要變更使用者的密碼。
   c. 在*存取*索引標籤上、允許使用者登入（選取*否*）、或視需要禁止使用者登入（選取*是*）。
   d. 在*群組*索引標籤上、視需要將使用者新增至群組或從群組中移除使用者。
   e. 視需要為每個區段選取*儲存變更*。

      由於快取、變更可能需要15分鐘才能生效。

複製本機使用者

您可以複製本機使用者、以更快建立新使用者。

步驟

1. 在使用者清單中、選取您要複製的使用者。
2. 選擇*複製使用者*。
3. 修改新使用者的下列欄位。
   - 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：此使用者用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。
   - 密碼：使用者登入時使用的密碼。
   - 確認密碼：在「密碼」欄位中輸入相同的密碼。
   - 拒絕存取：如果您選取*是*、此使用者就無法登入租戶帳戶、即使該使用者仍屬於一或多個群組。

     例如、您可以使用此功能暫時暫停使用者登入的能力。
4. 選擇*繼續*。
5. 選取一或多個本機群組。

   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。
6. 選取*建立使用者*。

   由於快取、變更可能需要15分鐘才能生效。

刪除本機使用者

您可以永久刪除不再需要存取StorageGRID 該經銷帳戶的本機使用者。

使用租戶管理程式、您可以刪除本機使用者、但不能刪除同盟使用者。您必須使用同盟識別來源來刪除同盟使用者。

步驟

1. 在使用者清單中、選取您要刪除之本機使用者的核取方塊。
2. 選取*「動作*」>*「刪除使用者*」。
3. 在確認對話方塊中、選取*刪除使用者*以確認您要從系統中刪除使用者。

   由於快取、變更可能需要15分鐘才能生效。

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。