控制對 StorageGRID 的存取

StorageGRID software

NetApp
July 23, 2026

目錄

控制對 StorageGRID 的存取

${post_edited_translations.segment}

您可以建立或匯入使用者群組，並為每個使用者群組指派權限，從而控制誰可以存取 StorageGRID 以及使用者可以執行哪些任務。您也可以選擇啟用單一登入 （SSO） 、建立用戶端憑證以及變更網格密碼。

控制對 **Grid Manager** 的存取

${post_edited_translations.segment}

使用 "${post_edited_translations.segment}" 可加快設定 "${post_edited_translations.segment}" 與 "使用者" 的速度，並允許使用者使用熟悉的認證資訊登入 StorageGRID。如果您使用 Active Directory、OpenLDAP 或 Oracle Directory Server，則可以設定身分識別聯盟。

${post_edited_translations.segment}

您可透過將不同的 "權限" 指派給每個群組，來決定每個使用者可以執行的工作。例如，您可能希望某個群組中的使用者能夠管理 ILM 規則，而另一個群組中的使用者則能執行維護工作。使用者必須至少屬於一個群組才能存取系統。

您可以選擇將某個群組設定為唯讀。唯讀群組中的使用者只能檢視設定和功能。無法在 Grid Manager 或 Grid Management API 中進行任何變更或執行任何操作。

啟用單一登入

StorageGRID 系統支援使用 Security Assertion Markup Language 2.0 (SAML 2.0) 標準的單一登入 (SSO)。在您 "設定並啟用 SSO" 之後，所有使用者都必須先通過外部身分識別供應商的驗證，才能存取 Grid Manager 、Tenant Manager、Grid Management API 或 Tenant Management API。本地使用者無法登入 StorageGRID。

${post_edited_translations.segment}

許多安裝和維護程序，以及下載 StorageGRID 恢復套件，都需要資源配置複雜密碼。下載 StorageGRID 系統的網格拓撲資訊和加密金鑰備份也需要此複雜密碼。您可以視需要 "更改密碼短語"。

${post_edited_translations.segment}

網格中的每個節點都有一個節點主控台密碼，您需要使用 SSH 以「admin」身分登入節點，或在虛擬機器/實體主控台連線上以 root 使用者身分登入。如有需要，您可以"變更節點主控台密碼"對每個節點執行此操作。

更改 StorageGRID 佈建通關密碼

使用此步驟變更 StorageGRID 佈建密碼。恢復、擴充和維護程序需要此密碼。下載包含網格拓撲資訊、網格節點主控台密碼和 StorageGRID 系統加密金鑰的恢復套件備份也需要此密碼。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您擁有維護或 root 存取權限。
- 您擁有目前的設定密碼。

關於此任務

許多安裝和維護程序都需要佈建密碼，以及 "下載恢復套件"。佈建密碼未列在 `Passwords.txt` 檔案中。請務必記錄佈建密碼，並將其保存在安全的位置。

步驟

1. 選擇 **Configuration** > **Access control** > **Grid passwords**。
2. 在 **Change provisioning passphrase** 下，選擇 **Make a change**
3. 請輸入您目前的佈建複雜密碼。
4. 請輸入新的密碼片語。密碼片語長度必須至少為 8 個字元，最多為 32 個字元。密碼片語區分大小寫。

   請將佈建密碼儲存在安全的位置。安裝、擴充和維護程序都需要用到它。

5. 重新輸入新的密碼短語，然後選擇 **Save**。

   配置密碼變更完成後，系統會顯示綠色成功橫幅。

6. 選擇 **Recovery Package**。
7. 輸入新的佈建密碼，以下載新的恢復套件。

   變更佈建密碼後，您必須立即下載新的恢復套件。恢復套件檔案可讓您在發生故障時還原系統。

在 StorageGRID 中變更節點主控台密碼

網格中的每個節點都有一個節點主控台密碼，用於登入節點。預設情況下，每個節點的密碼都是唯一的。您可以將每個節點的密碼變更為新的唯一密碼，也可以將所有節點的密碼變更為全域密碼。這些密碼儲存在恢復套件中。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"維護或 Root 存取權限"。
- 您擁有目前的設定密碼。

關於此任務

您可以使用節點主控台密碼透過 SSH 以「admin」身分登入節點，或透過虛擬機器/實體主控台連線以 root 使用者身分登入。您可以使用下列選項之一變更節點主控台密碼：

- 自動為每個節點套用隨機密碼
- ${post_edited_translations.segment}
- 為一個或多個節點指定並套用唯一密碼

密碼儲存在恢復套件中更新的 `Passwords.txt` 檔案中。密碼列在檔案的 Password 欄位中。

> 用於節點之間通訊的 SSH 金鑰 "${post_edited_translations.segment}" 與節點主控台密碼是分隔的。此程序不會變更 SSH 存取密碼。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Grid passwords**。
2. ${post_edited_translations.segment}

下載目前恢復套件

在變更節點主控台密碼之前，請先下載目前的恢復套件。如果任何節點的密碼變更程序失敗，您可以使用此檔案中的密碼。

步驟

1. 請輸入網格的佈建密碼。
2. ${post_edited_translations.segment}
3. 將恢復套件檔案 (`.zip`）複製到兩個安全且分隔的地點。

> 恢復套件檔案必須受到保護，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

4. 選擇 **Continue** 。

提供新密碼

1. 選擇您要使用的密碼變更方式。
   - 自動：StorageGRID 會自動為所有節點指派一個新的隨機主控台密碼。
   - 自訂：您提供主控台密碼。

自動

1. 選擇 **Continue** 。

自訂

1. 請選擇以下選項之一：
   - 全域主控台密碼：對所有節點套用相同的主控台密碼。
   - 唯一控制台密碼：在一個或多個節點上套用不同的密碼。
2. 如果您選取了 **Global console password**，請輸入您要用於所有節點的密碼。
3. 如果您選取了 **Unique console passwords**，請為一個或多個節點輸入唯一密碼。
4. 選擇 **Continue** 。

${post_edited_translations.segment}

1. 當出現確認對話方塊時，如果您已準備好讓 StorageGRID 開始變更節點主控台密碼，請選擇 **Yes**。

   此程序一旦開始便無法取消。

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
3. 開啟 `.zip` 檔案。
4. 確認您可以存取內容，包括 `Passwords.txt`檔案，其中包含新節點主控台密碼。
5. 將新的恢復套件檔案 (`.zip`) 複製到兩個安全、安全且分隔的位置。

   ${post_edited_translations.segment}

   您必須保護恢復檔案的安全，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

6. 選取此核取方塊，表示您已下載新的恢復套件並驗證其內容。
7. 選擇 **Continue** 。

   StorageGRID 更新每個節點的密碼。

   如果在更新過程中出現錯誤，進度條會顯示密碼變更失敗的節點數量。系統會自動對所有密碼變更失敗的節點重試更新過程。如果程序結束時仍有部分節點的密碼未變更，則會顯示 **Retry** 按鈕。

8. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. 解決問題。
   c. 選擇 **Retry**。

      重試只會變更先前密碼變更嘗試失敗的節點上的節點主控台密碼。

9. 當進度條顯示沒有剩餘更新時，選擇 **Finish**。
10. 在所有節點的節點主控台密碼變更完畢後，請刪除 您下載的第一個恢復套件。

變更 StorageGRID 管理節點的 SSH 存取密碼

變更管理節點的 SSH 存取密碼也會更新網格中每個節點的唯一內部 SSH 金鑰集。主要管理節點使用這些 SSH 金鑰，透過安全的無密碼驗證來存取節點。

使用 SSH 金鑰以 `admin`身分登入節點，或以 root 使用者身分登入虛擬機器或實體控制台連線。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"維護或 Root 存取權限"。
- 您擁有目前的設定密碼。

關於此任務

Admin 節點的新存取密碼以及每個節點的新內部金鑰，都儲存在恢復套件中的 `Passwords.txt` 檔案中。這些金鑰列在該檔案的 Password 欄中。

用於節點間通訊的 SSH 金鑰有個別的 SSH 存取密碼。此程序不會變更這些密碼。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Grid passwords**。
2. 在「Change SSH keys」下，選擇「Make a change」。

下載目前恢復套件

在變更 SSH 存取金鑰之前，請先下載目前的恢復套件。如果任何節點的金鑰變更程序失敗，您可以使用此檔案中的金鑰。

步驟

1. 請輸入網格的佈建密碼。
2. ${post_edited_translations.segment}
3. 將恢復套件檔案 (`.zip`）複製到兩個安全且分隔的地點。

> 恢復套件檔案必須受到保護，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

4. 選擇 **Continue** 。
5. ${post_edited_translations.segment}

> 此程序一旦開始便無法取消。

變更 SSH 存取金鑰

當變更 SSH 存取金鑰的程序開始時，會產生一個包含新金鑰的新恢復套件。然後，每個節點上的金鑰都會更新。

步驟

1. ${post_edited_translations.segment}
2. 當「下載新的恢復套件」按鈕啟用時，選取*下載新的恢復套件*，並將新的恢復套件檔案 (`.zip`) 儲存至兩個安全且分隔的位置。
3. 下載完成後：

   a. 開啟 `.zip` 檔案。

   b. 確認您可以存取內容，包括 `Passwords.txt`檔案，其中包含新的 SSH 存取金鑰。

   c. 將新的恢復套件檔案 (`.zip`) 複製到兩個安全、安全且分隔的位置。

   ${post_edited_translations.segment}

   恢復套件檔案必須受到保護，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

4. 等待每個節點上的金鑰更新，這可能需要幾分鐘。

   如果所有節點的金鑰都已更改，則會顯示綠色成功橫幅。

   如果在更新過程中出現錯誤，系統會顯示橫幅訊息，列出金鑰變更失敗的節點數量。系統會自動對所有金鑰變更失敗的節點重試更新過程。如果重試後仍有部分節點的金鑰未變更，則會顯示 **Retry** 按鈕。

   ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

   b. 解決問題。

   c. 選擇 **Retry**。

      重試只會變更先前金鑰變更嘗試失敗的節點上的 SSH 存取金鑰。

5. 在變更所有節點的 SSH 存取金鑰之後，請刪除 您下載的第一個恢復套件。
6. ${post_edited_translations.segment}

在 StorageGRID 中使用身分識別聯盟

${post_edited_translations.segment}

為 Grid Manager 設定身分識別聯盟

如果您希望在其他系統（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）中管理管理員群組和使用者，可以在 Grid Manager 中設定身分識別聯盟。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您已"特定存取權限"。
- 您使用的是 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作為身分供應商。

  如果您想使用未列出的 LDAP v3 服務，請聯絡技術支援。

- 如果您打算使用 OpenLDAP，則必須設定 OpenLDAP 伺服器。請參閱OpenLDAP 伺服器設定指南。
- 如果您打算啟用單一登入 （SSO），您已經查看了"${post_edited_translations.segment}"。
- 如果您打算使用傳輸層安全性協定 (TLS) 與 LDAP 伺服器進行通訊，則身分識別供應商將使用 TLS 1.2 或 1.3。請參閱"支援的傳出 TLS 連線加密套件"。

關於此任務

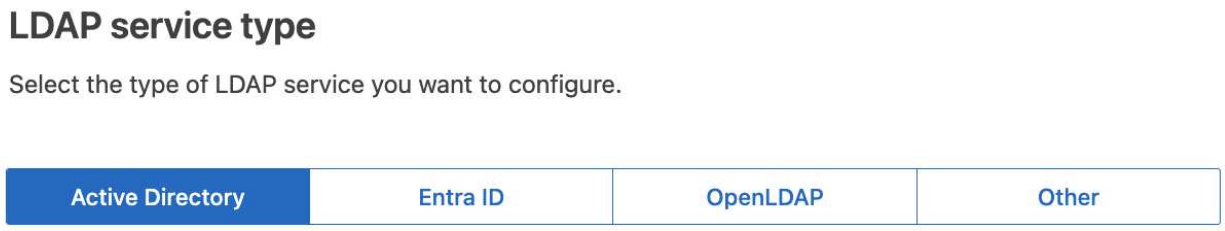
如果您想要從其他系統（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）匯入群組，可以為 Grid Manager 設定身分識別來源。您可以匯入以下類型的群組：

- 管理群組。管理群組中的使用者可以根據指派給該群組的管理權限，登入 Grid Manager 並執行工作。
- 租戶使用者群組適用於不使用自有身分來源的租戶。租戶群組中的使用者可以登入 Tenant Manager 並執行任務，具體任務取決於 Tenant Manager 中指派給該群組的權限。如需詳細資訊、請參閱 "建立租戶帳戶" 和 "使用租戶帳戶"。

輸入組態

步驟

1. 選擇 組態 > 存取控制 > 身分識別聯盟。
2. 選取 啟用身分識別聯盟。
3. 在 LDAP 服務類型部分，選擇要設定的 LDAP 服務類型。



   選擇「其他」以設定使用 Oracle Directory Server 的 LDAP 伺服器的值。

4. 如果您選擇了 **Other**，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：包含 LDAP 使用者唯一識別碼的屬性名稱。此屬性等效於 Active Directory 的 `sAMAccountName`和 `OpenLDAP` 的 `uid`。如果您正在設定 Oracle Directory Server，請輸入 `uid`。
   - 使用者 **UUID**：包含 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`。如果您正在設定 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，其中會忽略連字號。

- 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 `sAMAccountName` 和 OpenLDAP 的 `cn`。如果您正在設定 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。此屬性等效於 Active Directory 的 `objectGUID`和 `OpenLDAP 的 `entryUUID`。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個群組的指定屬性值必須為 32 位元十六進位數，格式可以是 16 個位元組或字串，其中連字元將被忽略。

5. 對於所有 LDAP 服務類型，請在「設定 LDAP 伺服器」部分輸入所需的 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：用於連接到 LDAP 伺服器的連接埠。

     STARTTLS 的預設 port 為 389，而 LDAPS 的預設 port 為 636。不過，只要您的防火牆設定正確，您可以使用任何 port。

   - 使用者名稱：將連接到 LDAP 伺服器的使用者辨別名稱 (DN) 完整路徑。

     對於 Active Directory，您也可以指定下級登入名稱或使用者主體名稱。

     ${post_edited_translations.segment}

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

   - ${post_edited_translations.segment}

     如果將來更改密碼，您必須在此頁面上更新密碼。

   - 群組基本 **DN**：您要搜尋群組之 LDAP 子樹狀結構的辨識名稱 （DN） 完整路徑。在 Active Directory 範例 （如下） 中，其辨識名稱相對於基本 DN （DC=storagegrid,DC=example,DC=com） 的所有群組，都可以用作同盟群組。

     ${post_edited_translations.segment}

   - 使用者基本 **DN**：要搜尋使用者的 LDAP 子樹的專有名稱 (DN) 的完整路徑。

     ${post_edited_translations.segment}

   - **Bind username format**（選用）：如果無法自動判斷模式，StorageGRID 應使用的預設使用者名稱模式。

建議提供 **Bind username format**，因為如果 StorageGRID 無法與服務帳戶連結，可允許使用者登入。

請輸入以下模式之一：

- **UserPrincipalName** 模式（**AD** 與 **Entra ID**）：`[USERNAME]@example.com`
- **Down-level logon name pattern** （**AD** 和 **Entra ID**）：`example\[USERNAME]`
- 辨別名稱模式：`CN=[USERNAME],CN=Users,DC=example,DC=com`

${post_edited_translations.segment}

6. ${post_edited_translations.segment}
   - 使用 **STARTTLS**：使用 STARTTLS 來保護與 LDAP 伺服器的通訊。對於 Active Directory、OpenLDAP 或其他 LDAP 伺服器，這是建議選項，但此選項不支援 Microsoft Entra ID。
   - 使用 **LDAPS**：LDAPS （LDAP over SSL） 選項會使用 TLS 建立與 LDAP 伺服器的連線。您必須為 Microsoft Entra ID 選擇此選項。
   - 請勿使用 **TLS**：StorageGRID 系統與 LDAP 伺服器之間的網路流量將不受保護。此選項不支援 Microsoft Entra ID。

   > 如果您的 Active Directory 伺服器強制執行 LDAP 簽名，則不支援使用「不使用 **TLS**」選項。您必須使用 STARTTLS 或 LDAPS。

7. ${post_edited_translations.segment}
   - 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。
   - **Use custom CA certificate**：使用自訂安全性憑證。

   ${post_edited_translations.segment}

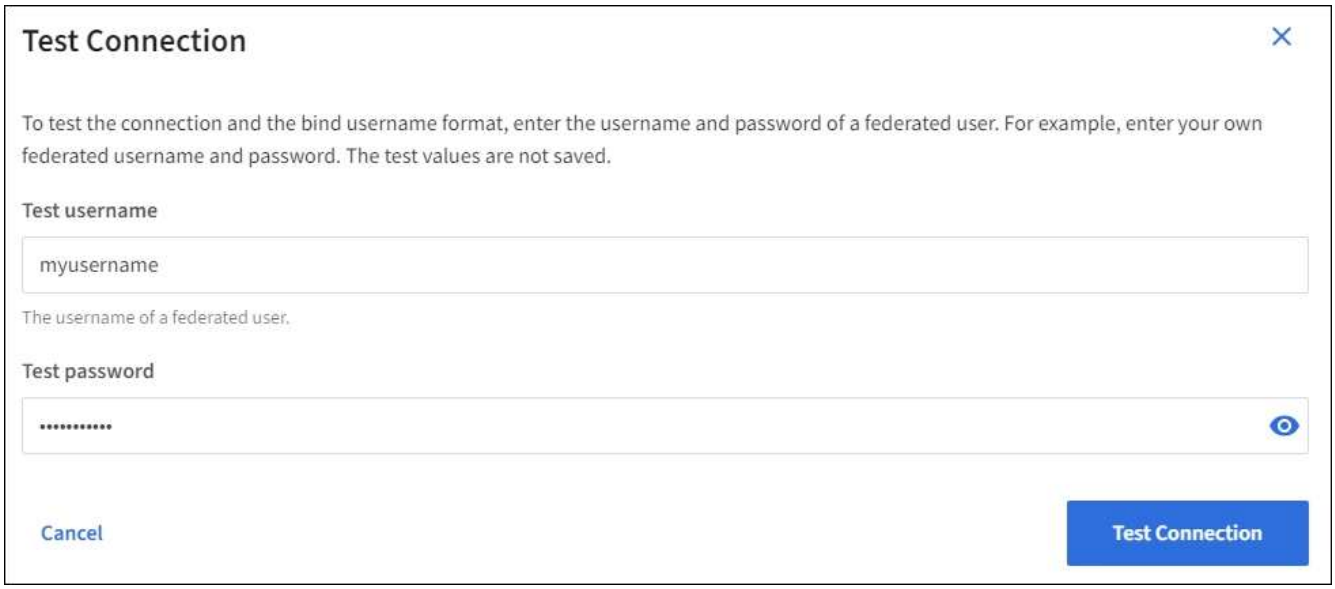
${post_edited_translations.segment}

輸入所有值後，必須先測試連線才能儲存組態。StorageGRID 會驗證 LDAP 伺服器的連線設定以及連結使用者名稱格式（如果您已提供）。

步驟

1. 選擇 **Test connection**。
2. ${post_edited_translations.segment}
   - 如果連線設定有效，則會顯示「測試連線成功」訊息。選擇*儲存*以儲存組態。
   - 如果連線設定無效，則會顯示「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. 如果您提供了連結使用者名稱格式，請輸入有效聯合使用者的使用者名稱和密碼。

   例如，請輸入您自己的使用者名稱和密碼。使用者名稱中請勿包含任何特殊字元，例如 @ 或 /。



- 如果連線設定有效，則會顯示「測試連線成功」訊息。選擇*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，則會顯示錯誤訊息。請解決所有問題並再次測試連線。

強制與身分來源同步

StorageGRID 系統會定期從識別來源同步聯盟群組與使用者。如果您想儘快啟用或限制使用者權限，可以強制開始同步。

步驟

1. 前往身分聯盟頁面。
2. ${post_edited_translations.segment}

   同步程序可能需要一些時間，視您的環境而定。

   ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以暫時或永久停用群組和使用者的身分聯合。停用身分聯合後，StorageGRID 與身分來源之間將不再通訊。但是，您已設定的所有設定都將保留，以便您日後可以輕鬆重新啟用身分聯合。

關於此任務

在停用身分聯合之前，您應該注意以下事項：

- 已加入聯盟的用戶將無法登入。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 如果單一登入 （SSO） 狀態為 已啟用 或 沙箱模式，則 啟用身分識別同盟 核取方塊會停用。您必須先將單一登入頁面上的 SSO 狀態設為 已停用，才能停用身分識別同盟。請參閱 "${post_edited_translations.segment}"。

步驟

1. 前往身分聯盟頁面。
2. ${post_edited_translations.segment}

OpenLDAP 伺服器設定指南

${post_edited_translations.segment}

> 對於非 Active Directory 或 Microsoft Entra ID 的身分識別來源，StorageGRID 不會自動封鎖在外部被停用之使用者的 S3 存取。若要封鎖 S3 存取，請刪除該使用者的任何 S3 金鑰，或將該使用者從所有群組中移除。

${post_edited_translations.segment}

應啟用 memberof 與 refint 重疊。如需詳細資訊，請參閱 "OpenLDAP 文件：版本 2.4 管理員指南" 中的反向群組成員資格維護說明。

${post_edited_translations.segment}

${post_edited_translations.segment}

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

${post_edited_translations.segment}

請參閱 "OpenLDAP 文件：版本 2.4 管理員指南" 中關於反向群組成員資格維護的資訊。

管理 StorageGRID 中的管理員群組

您可以建立管理員群組來管理一個或多個管理員使用者的安全性權限。使用者必須屬於某個群組，才能獲得對 StorageGRID 系統的存取權限。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。
- 如果您打算匯入聯合群組，則您已設定身分聯合，且該聯合群組已存在於已設定的身分來源中。

建立管理員群組

管理員群組可讓您決定哪些使用者可以存取 Grid Manager 和 Grid Management API 中的哪些功能和操作。

${post_edited_translations.segment}

步驟

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

${post_edited_translations.segment}

您可以建立本機群組或匯入聯合群組。

- 如果要為本機使用者指派權限，請建立本機群組。
- 建立聯合群組，從身分來源匯入使用者。

本地群組

步驟

1. 選擇*本機群組*。
2. 請輸入該群組的顯示名稱，您可以稍後視需要更新。例如，「Maintenance Users」或「ILM Administrators」。
3. 請為群組輸入唯一名稱，此名稱之後將無法更新。
4. 選擇 **Continue** 。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. 請輸入要匯入的群組名稱，務必與已設定的身分識別來源中顯示的名稱完全一致。
   - 對於 Active Directory 和 Microsoft Entra ID，請使用 sAMAccountName。
   - 對於 OpenLDAP，請使用 CN （Common Name）。
   - 對於另一個 LDAP，請使用 LDAP 伺服器的對應唯一名稱。
3. 選擇 **Continue** 。

${post_edited_translations.segment}

步驟

1. 對於*存取模式*，選擇群組中的使用者是否可以變更 Grid Manager 和 Grid Management API 中的設定並執行操作，或者他們是否只能檢視設定和功能。
   - ${post_edited_translations.segment}
   - 唯讀：使用者只能檢視設定和功能。無法對 Grid Manager 或 Grid Management API 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. 選取一或多個 "管理員群組權限"。

${post_edited_translations.segment}

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）

步驟

1. ${post_edited_translations.segment}

   如果您尚未建立本機使用者，則可以在不新增使用者的情況下儲存該群組。您可以在「使用者」頁面上將此群組新增至使用者。如需詳細資訊、請參閱 "管理使用者"。

2. ${post_edited_translations.segment}

檢視和編輯管理員群組

您可以檢視現有群組的詳細資訊、修改群組或複製群組。

- 若要檢視所有群組的基本資訊，請審查「群組」頁面上的表格。
- 若要檢視特定群組的所有詳細資訊或編輯群組，請使用 **Actions** 功能表或詳細資料頁面。

任務	操作選單	詳細資料頁面
檢視群組詳細資料	a. ${post_edited_translations.segment} b. 選取 **Actions** > **View group details**。	從表格中選擇群組名稱。
編輯顯示名稱（僅限本機群組）	a. ${post_edited_translations.segment} b. 選擇 **Actions** > **Edit group name**。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。	a. 選擇群組名稱以顯示詳細資訊。 b. 選擇編輯圖示 。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。
編輯存取模式或權限	a. ${post_edited_translations.segment} b. 選取 **Actions** > **View group details**。 c. ${post_edited_translations.segment} d. （可選）選擇或清除 "管理員群組權限"。 e. 選擇 **Save changes** 。	a. 選擇群組名稱以顯示詳細資訊。 b. ${post_edited_translations.segment} c. （可選）選擇或清除 "管理員群組權限"。 d. 選擇 **Save changes** 。

複製群組

步驟

1. ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

刪除群組

當您想要從系統中移除管理群組，並移除與該群組相關聯的所有權限時，可以刪除管理群組。刪除管理群組會將所有使用者從該群組中移除，但不會刪除這些使用者。

步驟

1. 在「群組」頁面中，選取要移除的每個群組的核取方塊。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

StorageGRID 中的管理員群組權限

建立管理使用者群組時，您可以選取一或多個權限，以控制對 Grid Manager 特定功能的存取。接著，您可以將每個使用者指派給一或多個此類管理群組，以決定該使用者可以執行的工作。

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 檢視儀表板
- 檢視節點頁面
- 檢視目前及已解決的警示
- 變更自己的密碼（僅限本機使用者）
- ${post_edited_translations.segment}

${post_edited_translations.segment}

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並執行作業，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，且有任何群組設定為 唯讀，則該使用者將對所有選取的設定和功能具有唯讀存取權限。

以下各節說明建立或編輯管理員群組時可以指派的權限。任何未明確提及的功能都需要 **Root access** 權限。

Root 存取

${post_edited_translations.segment}

${post_edited_translations.segment}

此權限可讓您存取 Tenants 頁面上的 **Change root password** 選項，從而控制哪些使用者可以變更租戶本機 root 使用者的密碼。啟用 S3 金鑰匯入功能時，此權限也用於移轉 S3 金鑰。沒有此權限的使用者將無法看到 **Change root password** 選項。

若要授予包含「變更 root 密碼」選項的「租戶」頁面的存取權限，也需要指派「租戶帳戶」權限。

ILM

${post_edited_translations.segment}

- 規則
- ${post_edited_translations.segment}
- 原則標籤
- 儲存池
- ${post_edited_translations.segment}
- 地區
- 物件中繼資料查詢

${post_edited_translations.segment}

${post_edited_translations.segment}

使用者必須擁有維護權限才能使用這些選項：

- 組態 > 存取控制：
  - 網格密碼
- 組態 > 網路：
  - ${post_edited_translations.segment}
- ${post_edited_translations.segment}
  - 取消委任
  - 擴充
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
- 維護 > 系統：
  - 恢復套件
  - 軟體更新
- 支援 > 工具：
  - ${post_edited_translations.segment}

沒有維護權限的使用者可以檢視這些頁面，但不能編輯：

- ${post_edited_translations.segment}
  - DNS 伺服器
  - Grid 網路

    - NTP 伺服器
- 維護 > 系統：
    - 授權
- 組態 > 網路：
    - ${post_edited_translations.segment}
- 組態 > 安全性：
    - 憑證
- 組態 > 監控：
    - 稽核與 syslog 伺服器

管理警報

此權限提供存取管理警示的選項。使用者必須擁有此權限才能管理靜默、警示通知和警示規則。

計量查詢

此權限允許存取：

- 支援 > 工具 > 計量 頁面
- ${post_edited_translations.segment}
- 包含計量的網格管理器儀表板卡片

物件中繼資料查詢

此權限提供對 **ILM** > 物件中繼資料查詢 頁面的存取。

${post_edited_translations.segment}

此權限允許存取以下額外的網格組態選項：

- ${post_edited_translations.segment}
    - ${post_edited_translations.segment}
- 組態 > 系統：
- ${post_edited_translations.segment}
    - 連結成本

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

租戶帳戶

此權限賦予您以下能力：

- 存取「租戶」頁面，您可以在此建立、編輯和移除租戶帳戶。
- ${post_edited_translations.segment}
- 檢視包含租戶詳細資訊的 Grid Manager 儀表板卡片

在 StorageGRID 中管理使用者

您可以檢視本機使用者和聯合使用者。您也可以建立本機使用者並將其指派至本機管理員群組，以決定這些使用者可以存取哪些 Grid Manager 功能。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。

建立本機使用者

您可以建立一個或多個本機使用者，並將每個使用者指派到一個或多個本機群組。群組的權限控制使用者可以存取哪些 Grid Manager 和 Grid Management API 功能。

您只能建立本機使用者。若要管理聯合使用者和群組，請使用外部身分來源。

Grid Manager 包含一個名為「root」的預先定義本機使用者。您無法移除 root 使用者。

如果啟用了單一登入 （SSO），則本機使用者無法登入 StorageGRID。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Admin users**。
2. 選取 **Create user**。

請輸入使用者憑證

步驟

1. 請輸入使用者的全名、唯一的使用者名稱和密碼。
2. 如果此使用者不應擁有 Grid Manager 或 Grid Management API 的存取權，可選擇選取「是」。
3. 選擇 **Continue** 。

分配到各個群組

步驟

1. （可選）將使用者指派到一個或多個群組，以決定使用者的權限。

如果您尚未建立群組，則可以在不選擇群組的情況下儲存使用者。您可以在「群組」頁面上將此使用者新增至群組。

如果使用者屬於多個使用者群組，則權限會累積。詳情請參閱"${post_edited_translations.segment}"。

2. 選擇 **Create user** ，然後選擇 **Finish** 。

檢視及編輯本機使用者

您可以檢視現有本機使用者和聯合使用者的詳細資訊。您可以修改本機使用者，例如變更使用者的全名、密碼或群組成員資格。您也可以暫時阻止使用者存取 Grid Manager 和 Grid Management API。

您只能編輯本機使用者。若要管理聯合使用者，請使用外部身分來源。

- 若要檢視所有本機和聯合使用者的基本資訊，請審查「使用者」頁面上的表格。
- 若要檢視特定使用者的所有詳細資訊、編輯本機使用者或變更本機使用者的密碼，請使用 **Actions** 功能表或詳細資料頁面。

  任何編輯都會在使用者下次登出並重新登入 Grid Manager 時生效。

  本機使用者可以使用 Grid Manager 橫幅中的「變更密碼」選項來變更自己的密碼。

任務	操作選單	詳細資料頁面
檢視使用者詳細資料	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。	從表格中選擇使用者的姓名。
編輯全名（僅限本機使用者）	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **Edit full name**。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選擇編輯圖示 。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。
拒絕或允許 StorageGRID 存取	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。 c. 選取「存取」索引標籤。 d. 選擇「是」可阻止使用者登入 Grid Manager 或 Grid Management API，選擇「否」可允許使用者登入。 e. 選擇 **Save changes** 。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選取「存取」索引標籤。 c. 選擇「是」可阻止使用者登入 Grid Manager 或 Grid Management API，選擇「否」可允許使用者登入。 d. 選擇 **Save changes** 。

任務	操作選單	詳細資料頁面
變更密碼（僅限本機使用者）	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。 c. 選擇「密碼」標籤。 d. 請輸入新密碼。 e. 選擇 **Change password**。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選擇「密碼」標籤。 c. 請輸入新密碼。 d. 選擇 **Change password**。
變更群組（僅限本機使用者）	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。 c. 選擇「群組」索引標籤。 d. （可選）選取群組名稱後的連結，即可在新瀏覽器標籤頁中檢視該群組的詳細資訊。 e. 選擇 **Edit groups** 以選擇不同的群組。 f. 選擇 **Save changes** 。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選擇「群組」索引標籤。 c. （可選）選取群組名稱後的連結，即可在新瀏覽器標籤頁中檢視該群組的詳細資訊。 d. 選擇 **Edit groups** 以選擇不同的群組。 e. 選擇 **Save changes** 。

匯入同盟使用者

您可以將一個或多個聯合使用者（最多 100 個使用者）直接匯入到「使用者」頁面。

步驟

1. 選擇 **Configuration** > **Access control** > **Admin users**。
2. 選取 **Import federated users**。
3. 輸入一個或多個聯合使用者的 UUID 或使用者名稱。

   對於多個條目，請將每個 UUID 或使用者名稱新增至新的一行。
4. 選取 **Import**。

   如果一個或多個使用者的匯入作業失敗，請執行下列步驟：

   a. 展開 **Users not imported** ，然後選擇 **Copy users** 。

   b. 選擇 **Previous** ，然後將複製的使用者貼上到 **Import federated users** 對話方塊中，重新嘗試匯入。

關閉*匯入聯合使用者*對話方塊後，成功匯入的使用者的聯合使用者資訊將顯示在「使用者」頁面上。

複製使用者

您可以複製現有使用者，建立具有相同權限的新使用者。

步驟

1. 選取該使用者的核取方塊。
2. 選擇 **Actions** > **Duplicate user**。
3. 完成複製使用者精靈。

刪除使用者

您可以刪除本機使用者，將其從系統中永久移除。

> 您無法刪除 root 使用者。

步驟

1. 在「使用者」頁面中，選取要移除的每個使用者的核取方塊。
2. 選擇*動作* > 刪除使用者。
3. 選取*刪除使用者*。

使用單一登入 (SSO)

了解 StorageGRID 單一登入

啟用單一登入 （SSO） 後，使用者只有在透過貴組織實作的 SSO 登入流程驗證其憑證後，才能存取 Grid Manager、Tenant Manager、Grid Management API 或 Tenant Management API。本機使用者無法登入 StorageGRID。

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 在網頁瀏覽器中輸入任何 StorageGRID 管理節點的完整網域名稱或 IP 位址。

   StorageGRID 登入頁面隨即出現。

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

   > 當您輸入租戶帳戶的完整 URL （即完整網域或 IP 位址，後跟 `/?accountId=20-digit-account-id`）時，不會顯示 StorageGRID 登入頁面。相反地，您會立即被重新導向至您組織的 SSO 登入頁面，您可以在該頁面 使用您的 SSO 憑證登入。

2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

◦ 若要存取 Tenant Manager，請輸入 20 位數的租戶帳戶 ID，或如果租戶出現在最近的帳戶清單中，請按名稱選擇租戶。

3. 選擇 **Sign in**

   StorageGRID 會將您重新導向至您組織的 SSO 登入頁面。例如：

4. 使用您的 SSO 憑證登入。

   如果您的 SSO 憑證正確：

   a. ${post_edited_translations.segment}
   b. StorageGRID 驗證驗證回應。
   c. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

啟用 **SSO** 後登出

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. 選擇「登出」。

   StorageGRID 登入頁面隨即顯示。最近使用的帳戶 下拉式功能表已更新，包含 **Grid Manager** 或租戶名稱，以便您日後能更快速地存取這些使用者介面。

   此表摘要說明如果您使用的是單一瀏覽器工作階段，在登出時會發生什麼事。如果您在多個瀏覽器工作階段中登入 StorageGRID，則必須個別登出所有的瀏覽器工作階段。

如果您已登入.....	然後您登出.....	您已登出.....
Grid Manager 位於一個或多個管理節點上	任何管理節點上的 Grid Manager	所有管理節點上的 Grid Manager *注意：*如果您使用 Entra ID 進行 SSO，則可能需要幾分鐘才能從所有管理節點登出。
${post_edited_translations.segment}	${post_edited_translations.segment}	所有管理節點上的租戶管理器
${post_edited_translations.segment}	Grid Manager	僅限 Grid Manager。您也必須從 Tenant Manager 登出才能登出單一登入 （SSO）。

StorageGRID 單一登入的要求和注意事項

在為 StorageGRID 系統啟用單一登入 （SSO） 之前，請審查相關要求和注意事項。

${post_edited_translations.segment}

StorageGRID 支援以下 SSO 身分供應商 (IdP)：

- Active Directory Federation Service （AD FS）
- ${post_edited_translations.segment}
- PingFederate

您必須先為您的 StorageGRID 系統設定身分識別同盟，然後才能設定 SSO 身分識別供應商。您用於身分識別同盟的 LDAP 服務類型會控制您可以實作的 SSO 類型。

${post_edited_translations.segment}	**${post_edited_translations.segment}**
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

${post_edited_translations.segment}

您可以使用以下任何版本的 AD FS：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Windows Server 2016 應該使用 "KB3201845 更新"或更高版本。

其他要求

- 傳輸層安全協定 (TLS) 1.2 或 1.3
- Microsoft .NET Framework，版本 3.5.1 或更高版本

Entra ID 的相關注意事項

如果您使用 Entra ID 作為 SSO 類型，且使用者的使用者主體名稱未使用 sAMAccountName 作為前綴，則當 StorageGRID 與 LDAP 伺服器斷開連線時，可能會出現登入問題。若要允許使用者登入，您必須還原與 LDAP 伺服器的連線。

伺服器憑證要求

預設情況下，StorageGRID 會在每個管理節點上使用管理介面憑證來保護對 Grid Manager、Tenant Manager、Grid Management API 和 Tenant Management API 的存取。當您為 StorageGRID 設定信賴方信任（AD FS

）、企業應用程式（Entra ID）或服務供應商連線（PingFederate）時，您將使用伺服器憑證作為 StorageGRID 請求的簽署憑證。

如果您尚未"已為管理介面設定自訂憑證"，請立即執行。安裝自訂伺服器憑證後，該憑證將用於所有管理節點，您可以將其用於所有 StorageGRID 信賴方信任、企業應用程式或 SP 連線。

> 不建議在信賴方信任、企業應用程式或 SP 連線中使用管理節點的預設伺服器憑證。如果節點發生故障並恢復後，系統會產生一個新的預設伺服器憑證。在登入已復原的節點之前，您必須使用新憑證更新信賴方信任、企業應用程式或 SP 連線。

您可以透過登入該節點的命令 shell 並前往 `/var/local/mgmt-api` 目錄，來存取 Admin Node 的伺服器憑證。自訂伺服器憑證的名稱為 `custom-server.crt`。該節點的預設伺服器憑證名稱為 `server.crt`。

連接埠需求

單一登入 (SSO) 在受限的 Grid Manager 或 Tenant Manager 連接埠上不可用。如果您希望使用者使用單一登入進行驗證，則必須使用預設的 HTTPS 連接埠 (443)。請參閱"${post_edited_translations.segment}"。

確認聯合使用者可以登入 **StorageGRID**

${post_edited_translations.segment}

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。
- ${post_edited_translations.segment}

步驟

1. 如果存在租戶帳戶，請確認沒有租戶使用自己的身分來源。

> 啟用單一登入 （SSO） 後，租戶管理員中設定的身分來源將會被 Grid Manager 中設定的身分來源覆寫。除非擁有 Grid Manager 身分來源的帳戶，否則屬於租戶身分來源的使用者將無法再登入。

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   a. 從 Grid Manager 中，選擇 **Configuration** > **Access control** > **Admin groups**。
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. 確認您可以以聯合群組使用者的身分重新登入 Grid Manager。
3. ${post_edited_translations.segment}
   a. 從 Grid Manager 中選擇 租戶。

b. ${post_edited_translations.segment}
c. ${post_edited_translations.segment}
d. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

e. ${post_edited_translations.segment}
f. 從 Tenant Manager 中選擇 **Access Management** > **Groups**。
g. ${post_edited_translations.segment}
h. ${post_edited_translations.segment}
i. 請確認您可以以聯合群組中的使用者身分重新登入租戶。

相關資訊

- "單一登入的要求和注意事項"
- "${post_edited_translations.segment}"
- "使用租戶帳戶"

在 **StorageGRID** 中設定 **SSO**

您可以依照 「Configure SSO」 精靈的指示並進入沙箱模式，在為所有 StorageGRID 使用者啟用單一登入 （SSO） 之前進行設定與測試。啟用 SSO 之後，您可以在需要變更或重新測試組態時返回沙箱模式。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- 您已為 StorageGRID 系統設定身分識別聯盟。
- 對於身分識別聯合 **LDAP** 服務類型，您可以根據計畫使用的 SSO 身分識別供應商選擇 Active Directory 或 Entra ID。

${post_edited_translations.segment}	**${post_edited_translations.segment}**
Active Directory Federation Service （AD FS）	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

關於此任務

啟用 SSO 後，當使用者嘗試登入管理節點時，StorageGRID 會向 SSO 身分供應商傳送驗證請求。SSO 身分供應商隨後會向 StorageGRID 傳送驗證回應，指示驗證要求是否成功。對於成功的請求：

- 來自 Active Directory 或 PingFederate 的回應包含使用者的通用唯一識別碼 (UUID)。

- Entra ID 的回應包含使用者主體名稱 (UPN)。

為了讓 StorageGRID （服務供應商）和 SSO 身分供應商能夠安全地就使用者身分驗證請求進行通訊，您需要完成以下任務：

1. 在 StorageGRID 中設定組態。
2. 使用 SSO 身分識別供應商的軟體，為每個管理節點建立信任憑證者關係（AD FS）、企業應用程式（Entra ID）或服務供應商（PingFederate）。
3. 返回 StorageGRID 以啟用 SSO。

沙盒模式便於進行此來回組態，並在啟用單一登入 (SSO) 之前測試所有設定。使用沙盒模式時，使用者無法使用 SSO 登入。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Single sign-on**。「單一登入」頁面隨即出現。

   如果「設定 SSO 設定」按鈕處於停用狀態，請確認您已將身分識別供應商設定為聯合身分識別來源。請參閱 "單一登入的要求和注意事項"。

2. 選取 **Configure SSO settings**。「提供身分供應商詳細資料」頁面隨即出現。

提供身分識別供應商詳細資訊

步驟

1. 從下拉清單中選取 **SSO** 類型。
2. ${post_edited_translations.segment}

   若要尋找同盟服務名稱，請前往 Windows Server Manager。選取 **Tools** > **AD FS Management**。從 Action 功能表中，選取 **Edit Federation Service Properties**。同盟服務名稱會顯示在第二個欄位中。

3. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

   - ${post_edited_translations.segment}

     如果變更 CA 憑證，請立即 "${post_edited_translations.segment}" 並測試是否能成功單一登入 Grid Manager。

4. 選擇 繼續。隨即顯示「提供信任憑證者識別碼」頁面。

${post_edited_translations.segment}

1. 根據您選擇的 SSO 類型，填寫「提供信賴方識別碼」頁面上的欄位。

Active Directory

a. 為 StorageGRID 指定*信賴方識別碼*。此值控制您在 AD FS 中為每個信賴方信任所使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示網格中每個管理節點的信賴方識別碼。

   > 您必須為 StorageGRID 系統中的每個管理節點建立信賴憑證者信任。為每個管理節點建立信賴憑證者信任，可確保使用者能夠安全地登入和登出任何管理節點。

b. ${post_edited_translations.segment}

Entra ID

a. 在「企業應用程式」區段中，指定 StorageGRID 的 企業應用程式名稱。此值控制您在 Entra ID 中為每個企業應用程式使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示系統中每個管理節點對應的企業應用程式名稱。

   > 您必須為 StorageGRID 系統中的每個管理節點建立一個企業應用程式。為每個管理節點配備企業應用程式可確保使用者可以安全地登入和登出任何管理節點。

b. 請按照 "在 Entra ID 中建立企業應用程式" 中的步驟，為表格中列出的每個管理節點建立企業應用程式。

c. 從 Entra ID 複製每個企業應用程式的同盟中繼資料 URL。然後，將此 URL 貼到 StorageGRID 中對應的*同盟中繼資料 URL* 欄位中。

d. 複製並貼上所有管理節點的聯盟中繼資料 URL 後，選取 儲存並進入沙盒模式。

PingFederate

a. 在「服務供應商 （SP）」部分，為 StorageGRID 指定 **SP** 連線 **ID**。此值控制您在 PingFederate 中每個 SP 連線所使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示系統中每個管理節點的 SP 連線 ID。

   > 您必須為 StorageGRID 系統中的每個管理節點建立一個 SP 連線。為每個管理節點建立 SP 連線可確保使用者可以安全地登入和登出任何管理節點。

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

c. ${post_edited_translations.segment}

設定信賴方信任、企業應用程式或 **SP** 連線

儲存組態並進入沙盒模式後，您可以完成並測試所選 SSO 類型的組態。

StorageGRID 可依需求保持在沙盒模式下。但是，只有同盟使用者和本機使用者才能登入。

Active Directory

步驟

1. 前往 Active Directory Federation Services （AD FS）。
2. 使用「設定 SSO」頁面上表格中顯示的每個信賴方識別碼，為 StorageGRID 建立一個或多個信賴方信任。

   ${post_edited_translations.segment}

   如需說明，請前往 "${post_edited_translations.segment}"。

Entra ID

步驟

1. ${post_edited_translations.segment}
2. 然後，對網格中的任何其他管理節點重複這些步驟：
   a. 登入節點。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 下載並儲存該節點的 SAML 中繼資料。
3. ${post_edited_translations.segment}
4. 請依照 "在 Entra ID 中建立企業應用程式" 中的步驟，將每個管理節點的 SAML 中繼資料檔案上傳至其對應的 Entra ID 企業應用程式。

PingFederate

步驟

1. ${post_edited_translations.segment}
2. 然後，對網格中的任何其他管理節點重複這些步驟：
   a. 登入節點。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 下載並儲存該節點的 SAML 中繼資料。
3. 前往 PingFederate。
4. "為 StorageGRID 建立一個或多個服務供應商 （SP） 連線"。使用每個管理節點的 SP 連線 ID （顯示在「設定 SSO」頁面上的表格中）以及您為該管理節點下載的 SAML 中繼資料。

   您必須為表中所示的每個管理節點建立一個 SP 連線。

測試組態

在對整個 StorageGRID 系統強制使用單一登入之前，請確認每個管理節點的單一登入和單一登出都已正確設定。

Active Directory

步驟

1. 在「設定 SSO」頁面上，找到精靈的「測試組態」步驟中的連結。

   URL 源自於您在「聯合服務名稱」欄位中輸入的值。

2. 選擇連結，或將 URL 複製並貼上到瀏覽器中，即可存取您的身分提供者的登入頁面。
3. 若要確認您可以使用 SSO 登入 StorageGRID，請選取 * 登入下列其中一個網站 *，選取您主要管理節點的信賴方識別碼，然後選取 * 登入 *。
4. 請輸入您的聯合使用者名稱和密碼。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
5. 重複這些步驟，以驗證網格中每個管理節點的 SSO 連線。

Entra ID

步驟

1. 前往 Azure 入口網站中的單一登入頁面。
2. 選擇 **Test this application**。
3. 請輸入聯合使用者的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
4. 重複這些步驟，以驗證網格中每個管理節點的 SSO 連線。

PingFederate

步驟

1. 在「設定 SSO」頁面中，選取「沙盒模式」訊息中的第一個連結。

   一次選擇並測試一個連結。

2. 請輸入聯合使用者的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
3. ${post_edited_translations.segment}

   如果看到「頁面已過期」訊息，請選擇瀏覽器中的「後退」按鈕，然後重新提交您的憑證。

啟用單一登入

${post_edited_translations.segment}

當啟用 SSO 時，所有使用者都必須使用 SSO 來存取 Grid Manager、Tenant Manager、Grid Management API 及 Tenant Management API。本機使用者無法再存取 StorageGRID。

步驟

1. 在設定 SSO 精靈的測試組態步驟中，選取 啟用 **SSO**。
2. 查看警告訊息，然後選擇 **Enable SSO**。

   現在已啟用單一登入。單一登入頁面隨即出現，且現在包含您剛才設定的 SSO 詳細資料。

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

如果您正在使用 Azure Portal，且您從用於存取 Entra ID 的相同電腦存取 StorageGRID，請確保 Azure Portal 使用者也是授權的 StorageGRID 使用者（已匯入至 StorageGRID 的聯合群組中的使用者），或在嘗試登入 StorageGRID 之前登出 Azure Portal。

在 **AD FS** 中為 **StorageGRID** 建立信賴方信任

您必須使用 Active Directory Federation Services （AD FS） 為系統中的每個管理節點建立信賴方信任。您可以使用 PowerShell 命令建立信賴方信任、從 StorageGRID 匯入 SAML 中繼資料，或手動輸入資料。

開始之前

- 您已為 StorageGRID 設定單一登入，並選取 **AD FS** 作為 SSO 類型。
- 您在 Grid Manager 中有 "進入沙盒模式"。
- 您知道系統中每個 Admin 節點的完整網域名稱（或 IP 位址）和信任憑證者識別碼。您可以在 StorageGRID 設定單一登入頁面的 Admin 節點詳細資料表中找到這些值。

  您必須為 StorageGRID 系統中的每個管理節點建立信賴憑證者信任。為每個管理節點建立信賴憑證者信任，可確保使用者能夠安全地登入和登出任何管理節點。

- ${post_edited_translations.segment}
- 您正在使用 AD FS Management 嵌入式管理單元，且您屬於 Administrators 群組。
- ${post_edited_translations.segment}

關於此任務

這些說明適用於 Windows Server 2016 AD FS。如果您使用的是不同版本的 AD FS，您會注意到程序中的些微差異。如果您有任何疑問，請參閱 Microsoft AD FS 文件。

使用 **Windows PowerShell** 建立信賴憑證者信任

您可以使用 Windows PowerShell 快速建立一個或多個信賴方信任。

步驟

1. 從 Windows 開始功能表中，以滑鼠右鍵選取 PowerShell 圖示，然後選取*以系統管理員身分執行*。

2. 在 PowerShell 命令提示字元下，輸入以下命令：

   `Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"` United States (US) - Company name: NetApp - Source text: `Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"` - The source text only contains an image placeholder tag. - According to the instructions, I must keep all `` tags exactly as they appear in the source text and return only the correct translation.

Output: `Add-AdfsRelyingPartyTrust -Name "*Admin_Node_Identifer*" -MetadataURL "https://*Admin_Node_FQDN*/api/saml-metadata"`_

+ 對於 ***`Admin_Node_Identifier`***，請輸入管理節點的信賴方識別碼，其內容必須與單一登入頁面上顯示的內容完全一致。例如， **`SG-DC1-ADM1`**。 針對 *`Admin_Node_FQDN`*，請輸入相同 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

1. ${post_edited_translations.segment}

   AD FS 管理工具出現。

2. ${post_edited_translations.segment}

   信賴方信任清單隨即出現。

3. 為新建立的信賴方信任新增存取控制原則：
   a. 找到您剛建立的信賴方信任。
   b. ${post_edited_translations.segment}
   c. 選擇存取控制原則。
   d. ${post_edited_translations.segment}
4. 為新建立的信賴方信任新增宣告發行原則：
   a. 找到您剛建立的信賴方信任。
   b. ${post_edited_translations.segment}
   c. 選擇 新增規則。
   d. ${post_edited_translations.segment}
   e. 在「設定規則」頁面上，輸入該規則的顯示名稱。

      ${post_edited_translations.segment}

   f. ${post_edited_translations.segment}
   g. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   h. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。
   i. 選擇 **Finish**，然後選擇 **OK**。
5. 確認中繼資料已成功匯入。
   a. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。

b. 確認「端點」、「識別碼」和「簽名」標籤上的欄位已填寫。

如果缺少中繼資料，請確認 Federation 中繼資料地址是否正確，或手動輸入值。

6. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。
7. 完成後，返回 StorageGRID 並"測試所有信賴憑證者信任"確認其組態是否正確。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 在 Windows Server 管理員中，選取 工具，然後選取 **AD FS Management**。
2. 在「操作」下，選擇 **Add Relying Party Trust**。
3. 在歡迎頁面上，選擇 **Claims aware**，然後選擇 **Start**。
4. 選擇「匯入有關依賴方的線上或區域網路上發佈的資料」。
5. 在「聯合中繼資料位址（主機名稱或 URL）」中，輸入此管理節點的 SAML 中繼資料的位置：

`https://Admin_Node_FQDN/api/saml-metadata`

針對 *`Admin_Node_FQDN`*，請輸入相同 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

6. ${post_edited_translations.segment}

> 輸入顯示名稱時，請使用管理節點的信賴方識別碼，該識別碼必須與 Grid Manager 單一登入頁面上顯示的識別碼完全一致。例如， `SG-DC1-ADM1`。

7. 新增聲明規則：
   a. ${post_edited_translations.segment}
   b. 選擇 新增規則：
   c. ${post_edited_translations.segment}
   d. 在「設定規則」頁面上，輸入該規則的顯示名稱。

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   g. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。
   h. 選擇 **Finish**，然後選擇 **OK**。
8. 確認中繼資料已成功匯入。
   a. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。
   b. 確認「端點」、「識別碼」和「簽名」標籤上的欄位已填寫。

如果缺少中繼資料，請確認 Federation 中繼資料地址是否正確，或手動輸入值。

9. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。
10. 完成後，請返回 StorageGRID 並"測試所有信賴憑證者信任"以確認其已正確設定。

手動建立信賴方信任

如果您選擇不匯入依賴方信託的資料，您可以手動輸入這些值。

步驟

1. 在 Windows Server 管理員中，選取 工具，然後選取 **AD FS Management**。
2. 在「操作」下，選擇 **Add Relying Party Trust**。
3. 在歡迎頁面上，選擇 **Claims aware**，然後選擇 **Start**。
4. 選擇 **Enter data about the relying party manually**，然後選擇 **Next**。
5. 完成信賴方信任嚮導：

   a. ${post_edited_translations.segment}

   為保持一致性，請使用管理節點的信賴方識別碼，該識別碼應與 Grid Manager 單一登入頁面上顯示的識別碼完全一致。例如， `SG-DC1-ADM1`。

   b. ${post_edited_translations.segment}

   c. ${post_edited_translations.segment}

   d. 輸入管理節點的 SAML 服務端點 URL：

   `https://Admin_Node_FQDN/api/saml-response`

   針對 *`Admin_Node_FQDN`*，請輸入 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

   e. ${post_edited_translations.segment}

   `*Admin_Node_Identifier*`_

   對於 *`Admin_Node_Identifier`*，請輸入管理節點的信賴方識別碼，其內容必須與單一登入頁面上顯示的內容完全一致。例如， `SG-DC1-ADM1`。

   f. 檢查設定，儲存信賴方信任，然後結束精靈。

   「編輯宣告簽發原則」對話方塊隨即出現。

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

   b. 在「設定規則」頁面上，輸入該規則的顯示名稱。

${post_edited_translations.segment}

c. ${post_edited_translations.segment}

d. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。

e. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。

f. 選擇 **Finish**，然後選擇 **OK**。

7. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。

8. ${post_edited_translations.segment}

a. 選擇 新增 **SAML**。

b. ${post_edited_translations.segment}

c. ${post_edited_translations.segment}

d. ${post_edited_translations.segment}

```
https://Admin_Node_FQDN/api/saml-logout
```

對於 *Admin_Node_FQDN*，請輸入管理節點的完整網域名稱。（如有必要，您也可以使用節點的 IP 位址。但是，如果您在此輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴方信任。）

a. 選擇 **OK** 。

9. 在「簽署」標籤上，指定此信賴方信任的簽署憑證：

a. 新增自訂憑證：

- 如果您有已上傳至 StorageGRID 的自訂管理憑證，請選擇該憑證。
- 如果沒有自訂憑證，請登入管理節點，前往管理節點的 `/var/local/mgmt-api`目錄，然後新增 `custom-server.crt`憑證檔案。

> 不建議使用管理節點的預設憑證 (`server.crt`。如果管理節點發生故障，恢復節點後將重新產生預設憑證，屆時您需要更新信賴方信任關係。

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

10. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。

11. 完成後，請返回 StorageGRID 並"測試所有信賴憑證者信任"以確認其已正確設定。

在 **Entra ID** 中為 **StorageGRID** 建立企業應用程式

您可以使用 Entra ID 為系統中的每個管理節點建立一個企業應用程式。

開始之前

- 您已開始為 StorageGRID 設定單一登入，並選擇了 **Entra ID** 作為 SSO 類型。
- 您在 Grid Manager 中有 "進入沙盒模式"。

- 您擁有系統中每個管理節點的 企業應用程式名稱。您可以從「設定 SSO」頁面上的管理節點詳細資料表格中複製這些值。

> 您必須為 StorageGRID 系統中的每個管理節點建立一個企業應用程式。為每個管理節點配備企業應用程式可確保使用者可以安全地登入和登出任何管理節點。

- 您擁有使用 Entra ID 建立企業應用程式的經驗。
- ${post_edited_translations.segment}
- 您在 Entra ID 帳戶中擁有以下角色之一：Global Administrator、Cloud Application Administrator、Application Administrator 或服務主體的擁有者。

存取 **Entra ID**

步驟

1. 登入 "${post_edited_translations.segment}"。
2. 導航至 "Entra ID"。
3. 選擇 "企業應用程式"。

${post_edited_translations.segment}

若要在 StorageGRID 中儲存 Entra ID 的單一登入組態，您必須使用 Entra ID 為每個管理節點建立一個企業應用程式。您將從 Entra ID 複製同盟中繼資料 URL，並將其貼到「設定單一登入」頁面上對應的 同盟中繼資料 **URL** 欄位中。

步驟

1. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. 選擇 **Create your own application**。
   c. 對於名稱，請輸入您從「設定 SSO」頁面上的「管理節點詳細資料」表中複製的*企業應用程式名稱*。
   d. 保持選取「整合您在資源庫中找不到的任何其他應用程式（非資源庫）」選項按鈕。
   e. 選擇 **Create** 。
   f. 在「2. 設定單一登入」方塊中選擇「開始使用」連結，或在左側邊欄中選擇「單一登入」連結。
   g. 選取 **SAML** 核取方塊。
   h. 複製 **App Federation Metadata Url**，您可以在 **Step 3 SAML Signing Certificate** 下找到它。
   i. 前往「設定 SSO」頁面，並將 URL 貼到與您使用的「企業應用程式名稱」對應的「同盟中繼資料 URL」欄位中。
2. 為每個管理節點貼上同盟中繼資料 URL 並對 SSO 組態進行所有其他必要的變更後，在「設定 SSO」頁面上選擇「儲存」。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
   a. 從管理節點登入 StorageGRID。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 選擇按鈕以下載該管理節點的 SAML 中繼資料。
   d. 儲存檔案，然後將其上傳到 Entra ID。

將 **SAML** 中繼資料上傳到每個企業應用程式

為每個 StorageGRID 管理節點下載 SAML 中繼資料檔案後，在 Entra ID 中執行下列步驟：

步驟

1. ${post_edited_translations.segment}
2. 對每個企業應用程式重複這些步驟：

   ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}
   b. 將 **Assignment required** 設為 **No** （除非您想單獨設定指派）。
   c. 前往單一登入頁面。
   d. ${post_edited_translations.segment}
   e. 選擇「上傳中繼資料檔案」按鈕，然後選擇您為對應的管理節點下載的 SAML 中繼資料檔案。
   f. 檔案載入完成後，選擇 **Save**，然後選擇 **X** 以關閉窗格。您將返回「使用 SAML 設定單一登入」頁面。
3. "${post_edited_translations.segment}"。

在 **PingFederate** 中為 **StorageGRID** 建立服務提供者連線

您需要使用 PingFederate 為系統中的每個管理節點建立一個服務供應商 （SP） 連線。為了加快此過程，您將從 StorageGRID 匯入 SAML 中繼資料。

開始之前

- ${post_edited_translations.segment}
- 您在 Grid Manager 中有 "進入沙盒模式"。
- 您擁有系統中每個管理節點的 **SP** 連線 **ID**。您可以在「設定 SSO」頁面的管理節點詳細資料表中找到這些值。
- 您已下載系統中每個管理節點的 **SAML** 中繼資料。
- 您有在 PingFederate Server 中建立 SP 連線的經驗。
- 您已取得 "管理員參考指南" PingFederate 伺服器端所需的檔案。PingFederate 文件中提供了詳細的逐步說明和解釋。
- 您已取得 "管理員權限" PingFederate 伺服器端所需的檔案。

關於此任務

這些說明摘要介紹如何將 PingFederate Server 10.3 版設定為 StorageGRID 的 SSO 供應商。如果您使用的是

其他版本的 PingFederate，您可能需要調整這些說明。有關您版本的詳細說明，請參閱 PingFederate Server 文件。

完成 **PingFederate** 中的先決條件

在您可以建立將用於 StorageGRID 的 SP 連線之前，您必須先在 PingFederate 中完成先決條件工作。當您設定 SP 連線時，將會使用來自這些先決條件的資訊。

建立資料儲存區

如果您尚未執行此操作，請建立資料儲存區以將 PingFederate 連線至 AD FS LDAP 伺服器。請使用您在 StorageGRID 中 "${post_edited_translations.segment}" 時所使用的值。

- 類型：目錄（LDAP）
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

建立密碼認證資料驗證器

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 搜尋篩選條件：sAMAccountName=${username}
- ${post_edited_translations.segment}

建立 **IdP** 介面卡執行個體

如果還沒有建立 IdP 介面卡執行個體，請建立一個。

步驟

1. 前往 **Authentication** > **Integration** > **IdP Adapters**。
2. 選擇 **Create New Instance**。
3. 在「類型」標籤上，選擇「HTML Form IdP Adapter」。
4. 在 IdP Adapter 標籤上，選擇「在『Credential Validators』新增一行」。
5. 選取您建立的 ${post_edited_translations.segment}。
6. 在「介面卡屬性」標籤上，為「**Pseudonym**」選擇「**username**」屬性。
7. 選取 **Save** 。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 前往 **Security** > **Signing & Decryption Keys & Certificates**。

2. 建立或匯入簽署憑證。

在 **PingFederate** 中建立 **SP** 連線

在 PingFederate 中建立 SP 連線時，您需要匯入從 StorageGRID 下載的管理節點 SAML 中繼資料。該中繼資料檔案包含您需要的許多特定值。

您必須為 StorageGRID 系統中的每個管理節點建立一個 SP 連線，以便使用者可以安全地登入和登出任何節點。請依照以下說明建立第一個 SP 連線。然後，前往 <<${post_edited_translations.segment}>> 建立您所需的任何其他連線。

選擇 **SP** 連線類型

步驟

1. 前往 **Applications** > **Integration** > **SP Connections**。
2. 選擇 **Create Connection**。
3. 選擇 **Do not use a template for this connection**。
4. ${post_edited_translations.segment}

匯入 **SP** 中繼資料

步驟

1. 在「匯入中繼資料」索引標籤上，選取 檔案。
2. 選擇您從管理節點的「設定 SSO」頁面下載的 SAML 中繼資料檔案。
3. ${post_edited_translations.segment}

   合作夥伴實體 ID 和連線名稱設定為 StorageGRID SP 連線 ID。（例如，10.96.105.200-DC1-ADM1-105-200）。基本 URL 是 StorageGRID 管理節點的 IP 位址。

4. 選擇 **Next** 。

${post_edited_translations.segment}

步驟

1. 在「瀏覽器 SSO」標籤中，選擇「設定瀏覽器 SSO」。
2. ${post_edited_translations.segment}
3. 選擇 **Next** 。
4. ${post_edited_translations.segment}
5. 在「斷言建立」標籤上，選取「設定斷言建立」。
   a. 在「身分映射」標籤上，選取 **Standard**。
   b. ${post_edited_translations.segment}
6. 如需延長合約，請選擇 **Delete** 以移除 `urn:oid`（未使用）。

對應介面卡執行個體

步驟

1. 在「驗證來源對應」標籤上，選擇 **Map New Adapter Instance**。
2. 在「介面卡執行個體」標籤上，選擇您建立的介面卡執行個體。
3. 在「映射方法」標籤上，選取*從資料儲存區擷取其他屬性*。
4. 在「屬性來源和使用者尋找」標籤上，選擇 **Add Attribute Source**。
5. 在「資料儲存區」標籤上，提供執行摘要並選擇您新增的 資料儲存區。
6. 在 LDAP 目錄搜尋標籤上：
   - 輸入 **Base DN**，該值應與您在 StorageGRID 中為 LDAP 伺服器輸入的值完全相符。
   - 在搜尋範圍中，選擇 **Subtree**。
   - 對於根物件類別，搜尋並新增下列屬性之一：**objectGUID** 或 **userPrincipalName**。
7. 在 LDAP 二進位屬性編碼類型標籤上，為 **objectGUID** 屬性選擇 **Base64**。
8. 在 LDAP 篩選器標籤上，輸入 **sAMAccountName=${username}**。
9. 在「屬性合約履行」標籤上，從「來源」下拉清單中選擇 **LDAP** （屬性），然後從「值」下拉清單中選擇 **objectGUID** 或 **userPrincipalName**。
10. 審查並儲存屬性來源。
11. 在「Failsave 屬性來源」標籤上，選取 中止 **SSO** 交易。
12. 審查摘要並選擇 **Done**。
13. 選擇 **Done**。

設定通訊協定設定

步驟

1. 在「**SP Connection**」>「**Browser SSO**」>「**Protocol Settings**」標籤上，選擇「**Configure Protocol Settings**」。
2. 在「Assertion Consumer Service URL」索引標籤上，接受預設值，這些預設值是從 StorageGRID SAML 中繼資料匯入的（Binding 為 **POST**，Endpoint URL 為 `/api/saml-response`）。
3. 在 SLO 服務 URL 索引標籤上，接受預設值，這些預設值是從 StorageGRID SAML 中繼資料匯入的（Binding 為 **REDIRECT**，`/api/saml-logout`為端點 URL）。
4. 在「允許的 SAML 綁定」標籤中，清除 **ARTIFACT** 和 **SOAP**。只需 **POST** 和 **REDIRECT**。
5. 在「簽署原則」標籤上，保持選取「要求對驗證要求進行簽署」和「始終簽署判斷提示」核取方塊。
6. 在「加密原則」索引標籤上，選取 **None**。
7. 審查摘要並選取 **Done** 以儲存通訊協定設定。
8. 審查摘要並選擇「完成」以儲存瀏覽器 SSO 設定。

設定認證資料

步驟

1. 在 SP Connection 標籤中，選擇「憑證」。

2. ${post_edited_translations.segment}
3. 選擇您建立或匯入的 簽署憑證。
4. ${post_edited_translations.segment}
    a. 在「信任模型」標籤上，選擇 **Unanchored**。
    b. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以複製第一個 SP 連線，為網格中的每個管理節點建立所需的 SP 連線。每個複本都需要上傳新的中繼資料。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
    a. ${post_edited_translations.segment}
    b. 選擇 **Choose File** 並上傳中繼資料。
    c. 選擇 **Next** 。
    d. 選取 **Save** 。
4. ${post_edited_translations.segment}
    a. ${post_edited_translations.segment}
    b. ${post_edited_translations.segment}
    c. ${post_edited_translations.segment}
    d. 選取 **Save** 。

停用 StorageGRID 中的 SSO

如果您不再需要此功能，可以停用單一登入 （SSO）。您必須先停用單一登入，然後才能停用身分識別聯盟。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。

步驟

1. 選擇 **Configuration** > **Access control** > **Single sign-on**。

    單一登入頁面隨即出現。

2. 選擇 停用單一登入。

3. ${post_edited_translations.segment}

   螢幕上出現警告訊息，指出本機使用者現在可以登入。

${post_edited_translations.segment}

暫時停用並重新啟用 **StorageGRID** 管理節點的 **SSO**

如果單一登入 （SSO） 系統故障，您可能無法登入 Grid Manager。在這種情況下，您可以暫時停用並重新啟用一個 Admin Node 的 SSO。若要停用並重新啟用 SSO，您必須存取該節點的命令 shell。

開始之前

- 您有"特定存取權限"。
- 您擁有 `Passwords.txt` 檔案。
- 您知道本機 root 使用者的密碼。

關於此任務

在您停用一個管理節點的 SSO 之後，您可以本機 root 使用者身分登入 Grid Manager。為了確保您的 StorageGRID 系統是安全的，您必須在登出後立即使用該節點的命令 shell 重新啟用管理節點上的 SSO。

> 停用單一 Admin Node 的 SSO 並不會影響網格中任何其他 Admin Node 的 SSO 設定。Grid Manager 中「單一登入」頁面上的「啟用 **SSO**」核取方塊仍會保持選取狀態，且所有現有的 SSO 設定都會保留，除非您對其進行更新。

步驟

1. ${post_edited_translations.segment}
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。

2. 執行下列命令：`disable-saml`

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

4. 透過網頁瀏覽器，存取同一管理節點上的 Grid Manager。

   由於 SSO 已停用，現在將顯示 Grid Manager 登入頁面。

5. ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
   a. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   b. ${post_edited_translations.segment}
   c. 選取 **Save** 。

      ${post_edited_translations.segment}

7. 如果您因為需要存取 Grid Manager 而暫時停用了 SSO：
   a. 執行您需要執行的任何工作。
   b. ${post_edited_translations.segment}
   c. 在 Admin 節點上重新啟用 SSO。您可以執行下列任一步驟：

      - 執行下列命令： `enable-saml`

        ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - 重啟網格節點： `reboot`

8. 透過網頁瀏覽器，從同一個管理節點存取 Grid Manager。
9. 確認 StorageGRID 登入頁面出現，且您必須輸入 SSO 憑證才能存取 Grid Manager。