控制對StorageGRID 的存取

StorageGRID software

NetApp
May 29, 2026

目錄

控制對StorageGRID 的存取

控制StorageGRID訪問

您可以透過建立或匯入群組和使用者並為每個群組分配權限來控制誰可以存取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。

控制對網格管理器的訪問

您可以透過從身分聯合服務匯入群組和使用者或設定本機群組和本機使用者來確定誰可以存取網格管理器和網格管理 API。

使用"身分聯合"使設定"群組"和"使用者"速度更快，並且允許使用者使用熟悉的憑證登入StorageGRID 。如果您使用 Active Directory、OpenLDAP 或 Oracle Directory Server，則可以設定身分聯合。

> 如果您想使用其他 LDAP v3 服務，請聯絡技術支援。

您可以透過指派不同的任務來確定每個使用者可以執行哪些任務"權限"到每個組。例如，您可能希望一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能夠執行維護任務。使用者必須至少屬於一個群組才能存取系統。

或者，您可以將群組配置為唯讀。只讀群組中的使用者只能查看設定和功能。他們無法在網格管理器或網格管理 API 中進行任何更改或執行任何操作。

啟用單一登入

StorageGRID系統支援使用安全性斷言標記語言 2.0 (SAML 2.0) 標準的單一登入 (SSO)。您先請"設定並啟用SSO"，所有使用者必須經過外部身分提供者的驗證，然後才能存取網格管理器、租用戶管理器、網格管理 API 或租用戶管理 API。本機使用者無法登入StorageGRID。

更改配置密碼

許多安裝和維護過程以及下載StorageGRID恢復包都需要設定密碼。下載StorageGRID系統的網格拓樸資訊和加密金鑰的備份也需要密碼。你可以"更改密碼"按要求。

更改節點控制台密碼

網格中的每個節點都有一個唯一的節點控制台密碼，您需要使用 SSH 以「管理員」身分登入節點，或以 VM/實體控制台連線上的 root 使用者身分登入。根據需要，您可以"更改節點控制台密碼"對於每個節點。

更改配置密碼

使用此程序更改StorageGRID配置密碼。恢復、擴充和維護過程都需要密碼。下載恢復包備份也需要密碼，其中包括網格拓撲資訊、網格節點控制台密碼和StorageGRID系統的加密金鑰。

開始之前

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

關於此任務

許多安裝和維護過程都需要配置密碼，並且"下載恢復包"。配置密碼未在 `Passwords.txt`文件。確保記錄配置密碼並將其保存在安全的地方。

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。
2. 在“更改配置密碼”下，選擇“進行更改”
3. 輸入您目前的設定密碼。
4. 輸入新密碼。密碼必須至少包含 8 個字符，但不能超過 32 個字符。密碼區分大小寫。
5. 將新的設定密碼儲存在安全的位置。它是安裝、擴充和維護過程所必需的。
6. 重新輸入新密碼，然後選擇*儲存*。

   當配置密碼變更完成後，系統將顯示綠色成功橫幅。

7. 選擇*恢復包*。
8. 輸入新的設定密碼來下載新的復原包。

   更改配置密碼後，您必須立即下載新的恢復包。如果發生故障，恢復包檔案可讓您恢復系統。

更改節點控制台密碼

網格中的每個節點都有一個唯一的節點控制台密碼，您需要該密碼才能登入該節點。使用這些步驟來變更網格中每個節點的每個唯一節點控制台密碼。

開始之前

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

關於此任務

使用節點控制台密碼透過 SSH 以「管理員」身分登入節點，或透過 VM/實體控制台連線以 root 使用者身分登入。更改節點控制台密碼程序會為網格中的每個節點建立新密碼，並將密碼儲存在更新的 `Passwords.txt`恢復包中的檔案。密碼列在 Passwords.txt 檔案的密碼欄位中。

節點間通訊使用的 SSH 金鑰有單獨的 SSH 存取密碼。此程序不會變更 SSH 存取密碼。

訪問嚮導

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。
2. 在*更改節點控制台密碼*下，選擇*進行更改*。

輸入設定密碼

步驟

1. 輸入您的網格的配置密碼。
2. 選擇*繼續*。

下載當前復原包

在變更節點控制台密碼之前，請下載目前的復原包。如果任何節點的密碼變更過程失敗，您可以使用此檔案中的密碼。

步驟

1. 選擇*下載恢復包*。
2. 複製復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

3. 選擇*繼續*。
4. 當確認對話方塊出現時，如果您準備好開始更改節點控制台密碼，請選擇*是*。

   一旦該過程開始，您就無法取消。

更改節點控制台密碼

當節點控制台密碼程序啟動時，將產生一個包含新密碼的新復原包。然後，在每個節點上更新密碼。

步驟

1. 等待新的恢復包生成，這可能需要幾分鐘。
2. 選擇*下載新的恢復包*。
3. 下載完成後：

   a. 打開 `.zip`文件。

   b. 確認您可以存取內容，包括 `Passwords.txt`文件，其中包含新的節點控制台密碼。

   c. 複製新的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

不要覆蓋舊的恢復包。

復原包檔案必須是安全的，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. 選取核取方塊表示您已下載新的復原套件並驗證了內容。
5. 選擇*更改節點控制台密碼*並等待所有節點更新新密碼。這可能需要幾分鐘。

   如果所有節點的密碼都已更改，則會出現綠色的成功橫幅。轉至下一步。

   如果更新過程中出現錯誤，橫幅訊息會列出密碼變更失敗的節點數。系統將自動在密碼變更失敗的任何節點上重試該過程。如果該過程結束時某些節點仍未更改密碼，則會出現「重試」按鈕。

   如果一個或多個節點的密碼更新失敗：

   a. 查看表中列出的錯誤訊息。
   b. 解決問題。
   c. 選擇*重試*。

   重試僅更改在前一次密碼變更嘗試中失敗的節點上的節點控制台密碼。

6. 更改所有節點的節點控制台密碼後，刪除您下載的第一個復原包。
7. 或者，使用*恢復包*鏈接下載新恢復包的附加副本。

更改管理節點的 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。主管理節點使用這些 SSH 金鑰透過安全、無密碼的身份驗證存取節點。

使用 SSH 金鑰以以下身分登入節點 `admin`或虛擬機器或實體控制台連接上的 root 使用者。

開始之前

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

關於此任務

管理節點的新存取密碼和每個節點的新內部金鑰儲存在 `Passwords.txt`恢復包中的檔案。密鑰列在該文件中的密碼列中。

節點間通訊使用的 SSH 金鑰有單獨的 SSH 存取密碼。這些不會因該過程而改變。

訪問嚮導

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。

2. 在*更改 SSH 金鑰*下，選擇*進行更改*。

下載當前復原包

在變更 SSH 存取金鑰之前，請下載目前的復原包。如果任何節點的金鑰變更過程失敗，您可以使用此文件中的金鑰。

步驟

1. 輸入您的網格的配置密碼。
2. 選擇*下載恢復包*。
3. 複製復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

> 復原包檔案必須是安全的，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*繼續*。
5. 當確認對話方塊出現時，如果您準備好開始變更 SSH 存取金鑰，請選擇「是」。

> 一旦該過程開始，您就無法取消。

變更 **SSH** 存取金鑰

當變更 SSH 存取金鑰程序開始時，將產生一個包含新金鑰的新復原包。然後，在每個節點上更新金鑰。

步驟

1. 等待新的恢復包生成，這可能需要幾分鐘。
2. 當「下載新的復原包」按鈕啟用時，選擇「下載新的復原包」並儲存新的復原包文件(`.zip`）到兩個安全、可靠且獨立的位置。
3. 下載完成後：
   a. 打開 `.zip`文件。
   b. 確認您可以存取內容，包括 `Passwords.txt`文件，其中包含新的 SSH 存取金鑰。
   c. 複製新的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

   > 不要覆蓋舊的恢復包。

   復原包檔案必須是安全的，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. 等待金鑰在每個節點上更新，這可能需要幾分鐘。

   如果所有節點的金鑰都發生了更改，則會出現綠色的成功橫幅。

   如果更新過程中出現錯誤，橫幅訊息會列出未能更改金鑰的節點數。系統將自動在密鑰更改失敗的任何節點上重試該過程。如果該過程結束時某些節點仍未更改金鑰，則會出現「重試」按鈕。

如果一個或多個節點的金鑰更新失敗：

a. 查看表中列出的錯誤訊息。
b. 解決問題。
c. 選擇*重試*。

   重試只會變更先前金鑰變更嘗試期間失敗的節點上的 SSH 存取金鑰。

5. 在所有節點的 SSH 存取金鑰變更後，刪除您下載的第一個復原包。
6. 或者，選擇 維護 > 系統 > 恢復包 來下載新恢復包的額外副本。

使用身分聯合

使用身份聯合可以更快地設定群組和用戶，並允許用戶使用熟悉的憑證登入StorageGRID。

為網格管理器配置身份聯合

如果您希望在另一個系統（例如 Active Directory、Azure Active Directory（Azure AD）、OpenLDAP 或 Oracle Directory Server）中管理管理員群組和用戶，則可以在網格管理器中設定身分合併。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您正在使用 Active Directory、Azure AD、OpenLDAP 或 Oracle Directory Server 作為身分提供者。

  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。看配置 OpenLDAP 伺服器的指南 。
- 如果您打算啟用單一登入 (SSO)，您已查看"單一登入的要求和注意事項"。
- 如果您打算使用傳輸層安全性 (TLS) 與 LDAP 伺服器進行通信，則身分提供者將使用 TLS 1.2 或 1.3。看"傳出 TLS 連線支援的密碼" 。

關於此任務

如果您想要從其他系統（例如 Active Directory、Azure AD、OpenLDAP 或 Oracle Directory Server）匯入群組，則可以為網格管理員設定身分來源。您可以匯入以下類型的群組：

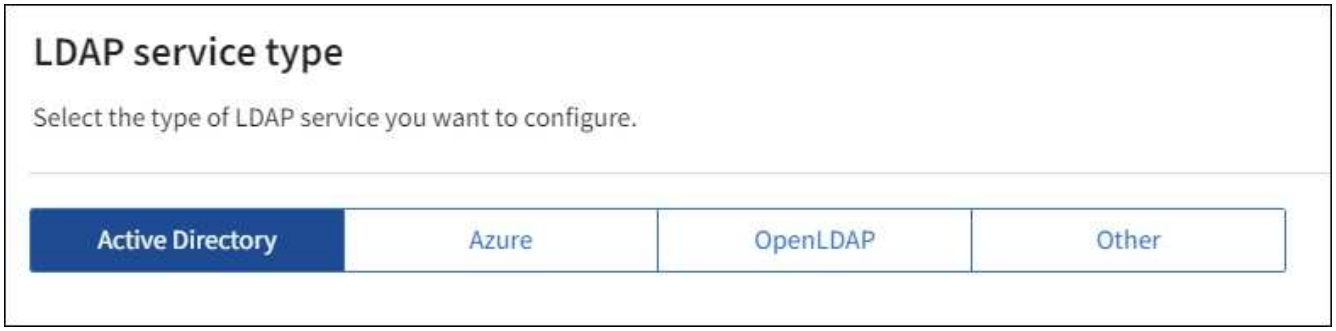
- 管理組。管理群組中的使用者可以登入網格管理器並根據指派給該群組的管理權限執行任務。
- 不使用自己的身分來源的租用戶的租用戶使用者群組。租用戶群組中的使用者可以登入租用戶管理員並根據租用戶管理員中指派給該群組的權限執行任務。看"建立租用戶帳戶"和"使用租用戶帳戶"了解詳情。

輸入配置

步驟

1. 選擇*配置* > 存取控制 > 身份聯合。

2. 選擇*啟用身份聯合*。
3. 在 LDAP 服務類型部分中，選擇要設定的 LDAP 服務類型。



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

4. 如果您選擇了"其他"，請填寫 LDAP 屬性部分中的欄位。否則，轉到下一步。
   - 使用者唯一名稱：包含 LDAP 使用者唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName`對於 Active Directory 和 `uid`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `uid`。
   - 使用者 **UUID**：包含 LDAP 使用者的永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID`對於 Active Directory 和 `entryUUID`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個使用者的指定屬性值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
   - 群組唯一名稱：包含 LDAP 群組唯一識別碼的屬性的名稱。此屬性相當於 `sAMAccountName`對於 Active Directory 和 `cn`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `cn`。
   - 群組 **UUID**：包含 LDAP 群組的永久唯一識別碼的屬性的名稱。此屬性相當於 `objectGUID`對於 Active Directory 和 `entryUUID`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個群組的指定屬性的值必須是 16 位元組或字串格式的 32 位元十六進位數，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 伺服器的完全限定網域名稱 (FQDN) 或 IP 位址。
   - 連接埠：用於連接 LDAP 伺服器的連接埠。

     STARTTLS 的預設連接埠是 389，LDAPS 的預設連接埠是 636。但是，只要您的防火牆配置正確，您就可以使用任何連接埠。

   - 使用者名稱：將連接到 LDAP 伺服器的使用者的專有名稱 (DN) 的完整路徑。

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

     指定的使用者必須具有列出群組和使用者以及存取以下屬性的權限：

     - `sAMAccountName`或者 `uid`
     - `objectGUID`， `entryUUID` ， 或者 `nsuniqueid`
     - `cn`

- `memberOf`或者 `isMemberOf`
- 活動目錄： `objectSid` ， `primaryGroupID` ， `userAccountControl` ，和 `userPrincipalName`
- 蔚藍： `accountEnabled`和 `userPrincipalName`

◦ 密碼：與使用者名稱關聯的密碼。

> 如果您將來更改密碼，則必須在此頁面上更新。

◦ 群組基礎 **DN**：您要搜尋群組的 LDAP 子樹的可分辨名稱 (DN) 的完整路徑。在 Active Directory 範例（如下）中，所有可分辨名稱相對於基本 DN（DC=storagegrid、DC=example、DC=com）的群組都可以用作聯合群組。

> *群組唯一名稱*值在其所屬的*群組基本 DN*內必須是唯一的。

◦ 使用者基礎 **DN**：您要搜尋使用者的 LDAP 子樹的可分辨名稱 (DN) 的完整路徑。

> *使用者唯一名稱*值在其所屬的*使用者基本 DN*內必須是唯一的。

◦ 綁定使用者名稱格式（選用）：如果無法自動確定模式， StorageGRID應使用預設使用者名稱模式。

建議提供*綁定使用者名稱格式*，因為如果StorageGRID無法與服務帳戶綁定，它可以允許使用者登入。

輸入以下模式之一：

- **UserPrincipalName** 模式（**Active Directory** 和 **Azure**）： `[USERNAME]@*example*.com`
- 下級登入名稱模式（**Active Directory** 和 **Azure**）： `*example*\[USERNAME]`
- 可分辨名稱模式： `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  完全按照書寫方式包含 **[USERNAME]**。

6. 在傳輸層安全性 (TLS) 部分中，選擇一個安全性設定。

◦ 使用 **STARTTLS**：使用 STARTTLS 確保與 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（透過 SSL 的 LDAP）選項使用 TLS 建立與 LDAP 伺服器的連線。您必須為 Azure 選擇此選項。

◦ 請勿使用 **TLS**： StorageGRID系統和 LDAP 伺服器之間的網路流量將不安全。 Azure 不支援此選項。

> 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. 如果您選擇了 STARTTLS 或 LDAPS，請選擇用於保護連線的憑證。

◦ 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。

◦ 使用自訂 **CA** 憑證：使用自訂安全性憑證。

如果選擇此設置，請將自訂安全性憑證複製並貼上到 CA 憑證文字方塊中。

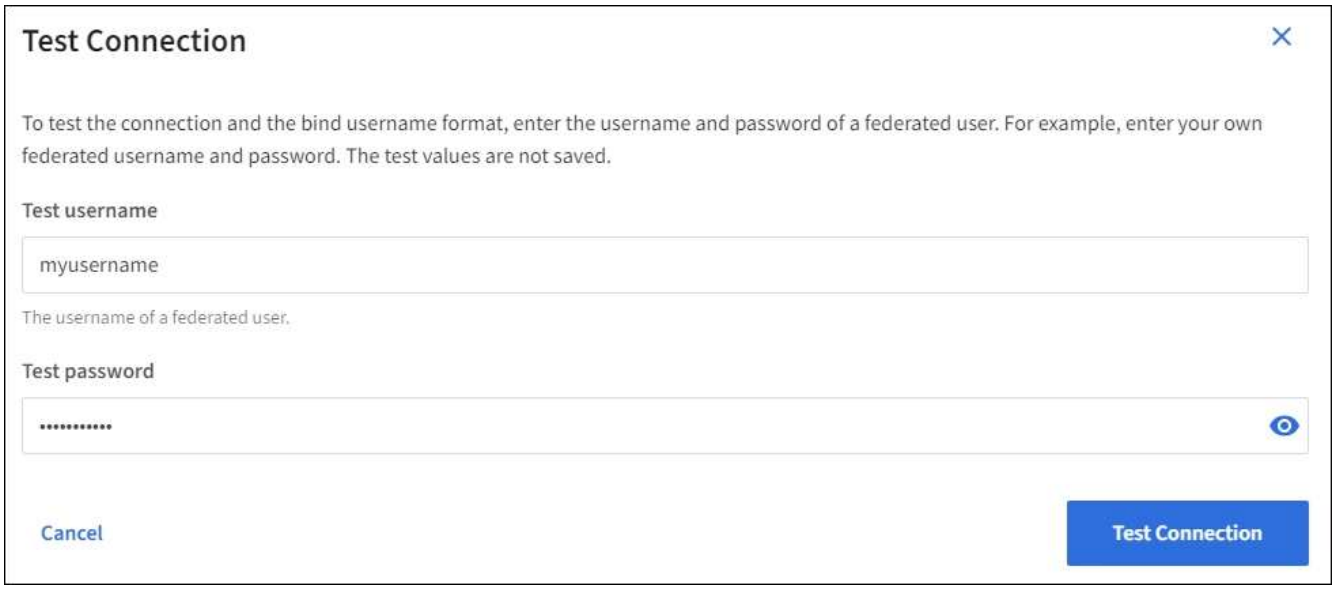
測試連接並儲存配置

輸入所有值後，必須先測試連接，然後才能儲存配置。如果您提供了 LDAP 伺服器的連線設定和綁定使用者名稱格式， StorageGRID會驗證該設定。

步驟

1. 選擇*測試連線*。
2. 如果您沒有提供綁定使用者名稱格式：
   - 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
   - 如果連線設定無效，則會出現「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. 如果您提供了綁定使用者名稱格式，請輸入有效聯合使用者的使用者名稱和密碼。

   例如，輸入您自己的使用者名稱和密碼。用戶名中不要包含任何特殊字符，例如 @ 或 /。



   - 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
   - 如果連線設定、綁定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。解決任何問題並再次測試連接。

強制與身分來源同步

StorageGRID系統會定期從身分識別來源同步聯合群組和使用者。如果您想盡快啟用或限制使用者權限，您可以強制啟動同步。

步驟

1. 前往身份聯合頁面。
2. 選擇頁面頂部的*同步伺服器*。

   同步過程可能需要一些時間，具體取決於您的環境。

如果從身分來源同步聯合群組和使用者時出現問題，則會觸發*身分聯合同步失敗*警報。

禁用身份聯合

您可以暫時或永久停用群組和使用者的身份聯合。當身分聯合被停用時， StorageGRID和身分來源之間就沒有通訊。但是，您配置的任何設定都會保留，以便您將來可以輕鬆地重新啟用身份聯合。

關於此任務

在停用身分聯合之前，您應該注意以下事項：

- 聯合用戶將無法登入。
- 目前已登入的聯合用戶將保留對StorageGRID系統的存取權限，直到其會話過期，但會話過期後他們將無法登入。
- StorageGRID系統和身分來源之間不會發生同步，並且不會針對未同步的帳戶發出警報。
- 如果單一登入 (SSO) 設定為 已啟用 或 沙盒模式，則 啟用身分聯合 核取方塊將會停用。在停用身分聯合之前，單一登入頁面上的 SSO 狀態必須為 已停用。看"停用單一登入" 。

步驟

1. 前往身份聯合頁面。
2. 取消選取「啟用身份聯合」複選框。

配置 **OpenLDAP** 伺服器的指南

如果您想要使用 OpenLDAP 伺服器進行身份聯合，則必須在 OpenLDAP 伺服器上設定特定設定。

對於非 ActiveDirectory 或 Azure 的識別來源， StorageGRID不會自動阻止外部停用的使用者存取 S3。若要封鎖 S3 訪問，請刪除使用者的所有 S3 金鑰或從所有群組中刪除該使用者。

Memberof 和 **refint** 覆蓋

應該啟用 memberof 和 refint 覆蓋。有關詳細信息，請參閱http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文件：版本 2.4 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，請確保幫助中提到的使用者名字段已索引，以獲得最佳效能。

請參閱有關反向群組成員資格維護的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文件：版本 2.4 管理員指南"^]。

管理管理員群組

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權限。使用者必須屬於某個群組才能被授予對StorageGRID系統的存取權限。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 如果您計劃匯入聯合群組，則您已配置身分聯合，且聯合群組已存在於配置的身分來源中。

建立管理員群組

管理群組可讓您確定哪些使用者可以存取網格管理器和網格管理 API 中的哪些功能和操作。

訪問嚮導

步驟

1. 選擇 配置 > 存取控制 > 管理群組。
2. 選擇*建立群組*。

選擇群組類型

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。
- 建立聯合群組以從身分來源匯入使用者。

本地群組

步驟

1. 選擇*本機群組*。
2. 輸入群組的顯示名稱，您可以根據需要稍後更新。例如，「維護使用者」或「ILM 管理員」。
3. 為該群組輸入一個唯一的名稱，該名稱以後無法更新。
4. 選擇*繼續*。

聯合組

步驟

1. 選擇*聯合組*。
2. 輸入要匯入的群組的名稱，與設定的身份來源中顯示的名稱完全一致。
   - 對於 Active Directory 和 Azure，使用 sAMAccountName。
   - 對於 OpenLDAP，使用 CN（通用名稱）。
   - 對於另一個 LDAP，請使用 LDAP 伺服器的適當唯一名稱。
3. 選擇*繼續*。

管理群組權限

步驟

1. 對於*存取模式*，選擇群組中的使用者是否可以更改設定並在網格管理器和網格管理 API 中執行操作，或者他們是否只能查看設定和功能。
   - 讀寫（預設）：使用者可以更改設定並執行其管理權限允許的操作。
   - 只讀：使用者只能查看設定和功能。他們無法在網格管理器或網格管理 API 中進行任何更改或執行任何操作。本機只讀使用者可以更改自己的密碼。

   如果使用者屬於多個群組，並且任何群組設定為*只讀*，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

2. 選擇一個或多個"管理員群組權限"。

   您必須為每個群組指派至少一個權限；否則，屬於該群組的使用者將無法登入StorageGRID。

3. 如果您正在建立本機群組，請選擇*繼續*。如果您正在建立聯合群組，請選擇*建立群組*和*完成*。

新增使用者（僅限本地群組）

步驟

1. 或者，為此群組選擇一個或多個本機使用者。

   如果您尚未建立本機用戶，則可以儲存群組而不新增使用者。您可以在「使用者」頁面上將此群組新增至使用者。看"管理用戶"了解詳情。

2. 選擇*建立群組*和*完成*。

檢視和編輯管理員群組

您可以查看現有群組的詳細資訊、修改群組或複製群組。

- 要查看所有群組的基本信息，請查看群組頁面上的表格。
- 若要查看特定群組的所有詳細資訊或編輯群組，請使用*操作*功能表或詳細資料頁面。

任務	操作選單	詳細資訊頁面
查看群組詳情	a. 選取該組的複選框。 b. 選擇*動作* > 查看群組詳情。	在表中選擇組名。
編輯顯示名稱（僅限本機群組）	a. 選取該組的複選框。 b. 選擇*操作* > 編輯群組名稱。 c. 輸入新名稱。 d. 選擇“儲存變更”。	a. 選擇群組名稱以顯示詳細資訊。 b. 選擇編輯圖標。 c. 輸入新名稱。 d. 選擇“儲存變更”。
編輯存取模式或權限	a. 選取該組的複選框。 b. 選擇*動作* > 查看群組詳情。 c. 或者，更改群組的存取模式。 d. （可選）選擇或清除"管理員群組權限"。 e. 選擇“儲存變更”。	a. 選擇群組名稱以顯示詳細資訊。 b. 或者，更改群組的存取模式。 c. （可選）選擇或清除"管理員群組權限"。 d. 選擇“儲存變更”。

複製群組

步驟

1. 選取該組的複選框。
2. 選擇*動作* > 複製群組。
3. 完成複製組精靈。

刪除群組

當您想要從系統中刪除該群組時，您可以刪除該管理員群組，並刪除與該群組相關的所有權限。刪除管理員群組會從群組中刪除所有用戶，但不會刪除用戶。

步驟

1. 在「群組」頁面中，選取要刪除的每個群組的核取方塊。
2. 選擇*動作* > 刪除群組。
3. 選擇*刪除群組*。

管理員群組權限

建立管理員使用者群組時，您可以選擇一個或多個權限來控制對網格管理器特定功能的存取。然後，您可以將每個使用者指派到一個或多個管理群組，以確定該使用者可以執行哪些任務。

您必須為每個群組指派至少一個權限；否則，屬於該群組的使用者將無法登入網格管理器或網格管理 API。

預設情況下，屬於具有至少一個權限的群組的任何使用者都可以執行以下任務：

- Sign in入網格管理器
- 查看儀表板
- 查看節點頁面
- 查看當前和已解決的警報
- 更改自己的密碼（僅限本地用戶）
- 查看配置和維護頁面上提供的某些信息

權限與存取模式的交互

對於所有權限，群組的*存取模式*設定決定使用者是否可以變更設定和執行操作，或者是否只能查看相關設定和功能。如果使用者屬於多個群組，並且任何群組設定為*只讀*，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

以下部分描述了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 存取*權限。

Root 存取權限

此權限提供對所有網格管理功能的存取。

更改租用戶 root 密碼

此權限提供對租用戶頁面上的*更改 root 密碼*選項的存取權限，讓您可以控制誰可以更改租用戶本地 root 使用者的密碼。啟用 S3 金鑰導入功能時，此權限也用於遷移 S3 金鑰。沒有此權限的使用者無法看到*更改 root 密碼*選項。

> 若要授予包含「變更根密碼」選項的「租用戶」頁面的存取權限，也需指派「租用戶帳號」權限。

電網拓撲頁面配置

此權限提供對 **SUPPORT** > **Tools** > **Grid topology** 頁面上的配置標籤的存取權限。

> 網格拓撲頁面已被棄用，並將在未來版本中刪除。

工業光魔

此權限提供對以下 **ILM** 選單選項的存取：

- 規則
- 政策
- 策略標籤
- 儲存池
- 儲存等級
- 區域
- 對像元資料查找

使用者必須具備*其他電網配置*和*電網拓撲頁面配置*權限才能管理儲存等級。

維護

使用者必須具有維護權限才能使用這些選項：

- 配置 > 存取控制：
  - 電網密碼
- 配置 > 網路：
  - S3 端點域名
- 維護 > 任務：
  - 退休
  - 擴張
  - 對象存在性檢查
  - 恢復
- 維護 > 系統：
  - 恢復包
  - 軟體更新
- 支援 > 工具：
  - 紀錄

沒有維護權限的使用者可以查看但不能編輯以下頁面：

- 維護 > 網路：
  - DNS 伺服器
  - 網格網絡
  - NTP 伺服器

- 維護 > 系統：
  - 執照
- 配置 > 網路：
  - S3 端點域名
- 配置 > 安全：
  - 證書
- 配置 > 監控：
  - 審計和系統日誌伺服器

管理警報

此權限提供對管理警報選項的存取。使用者必須擁有此權限才能管理靜默、警報通知和警報規則。

指標查詢

此權限提供以下存取權限：

- 支援 > 工具 > *指標*頁面
- 使用網格管理 API 的 **Metrics** 部分自訂 Prometheus 指標查詢
- 包含指標的網格管理器儀表闆卡

對像元資料查找

此權限提供對 **ILM** > 物件元資料查找 頁面的存取權限。

其他電網配置

此權限提供對其他網格配置選項的存取。

要查看這些附加選項，使用者還必須具有*網格拓撲頁面配置*權限。

- 工業光魔（ILM）：
  - 儲存等級
- 配置 > 系統：
- 支援 > 其他：
  - 鏈路成本

儲存設備管理員

此權限提供：

- 透過網格管理器存取儲存設備上的 E 系列SANtricity系統管理器。

- 能夠在支援這些操作的裝置的「管理磁碟機」標籤上執行故障排除和維護任務。

租戶帳戶

此權限提供以下功能：

- 造訪租戶頁面，您可以在其中建立、編輯和刪除租戶帳戶
- 查看現有的流量分類策略
- 查看包含租戶詳細資訊的網格管理器儀表闆卡

管理用戶

您可以查看本地用戶和聯合用戶。您還可以建立本機使用者並將其指派到本機管理員群組，以確定這些使用者可以存取哪些網格管理器功能。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

建立本地用戶

您可以建立一個或多個本機用戶，並將每個用戶指派到一個或多個本機群組。此群組的權限控制使用者可以存取哪些網格管理器和網格管理 API 功能。

您只能建立本機使用者。使用外部身分來源來管理聯合使用者和群組。

網格管理器包含一個預先定義的本機用戶，名為「root」。您不能刪除 root 使用者。

如果啟用單一登入 (SSO)，本機使用者將無法登入StorageGRID。

訪問嚮導

步驟

1. 選擇 配置 > 存取控制 > 管理員使用者。
2. 選擇*建立使用者*。

輸入使用者憑證

步驟

1. 輸入使用者的全名、唯一的使用者名稱和密碼。
2. 或者，如果此使用者不應存取網格管理器或網格管理 API，請選擇「是」。
3. 選擇*繼續*。

分配給群組

步驟

1. 或者，將使用者指派到一個或多個群組以確定使用者的權限。

   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群組，則權限是累積的。看"管理管理員群組"了解詳情。

2. 選擇*建立使用者*並選擇*完成*。

查看和編輯本地用戶

您可以查看現有本地用戶和聯合用戶的詳細資訊。您可以修改本機使用者以變更使用者的全名、密碼或群組成員身分。您也可以暫時阻止使用者存取網格管理器和網格管理 API。

您只能編輯本機使用者。使用外部身分來源來管理聯合使用者。

- 要查看所有本地和聯合用戶的基本信息，請查看“用戶”頁面上的表格。
- 若要查看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*操作*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網格管理器時套用。

  本機使用者可以使用網格管理器橫幅中的「變更密碼」選項來變更自己的密碼。

任務	操作選單	詳細資訊頁面
查看用戶詳細信息	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。	在表中選擇用戶的姓名。
編輯全名（僅限本地用戶）	a. 選取使用者的複選框。 b. 選擇*動作* > 編輯全名。 c. 輸入新名稱。 d. 選擇“儲存變更”。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇編輯圖標。 c. 輸入新名稱。 d. 選擇“儲存變更”。
拒絕或允許StorageGRID訪問	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。 c. 選擇“訪問”選項卡。 d. 選擇「是」以阻止使用者登入網格管理員或網格管理 API，或選擇「否」以允許使用者登入。 e. 選擇“儲存變更”。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇“訪問”選項卡。 c. 選擇「是」以阻止使用者登入網格管理員或網格管理 API，或選擇「否」以允許使用者登入。 d. 選擇“儲存變更”。

任務	操作選單	詳細資訊頁面
更改密碼（僅限本機用戶）	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。 c. 選擇密碼選項卡。 d. 輸入新密碼。 e. 選擇*更改密碼*。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇密碼選項卡。 c. 輸入新密碼。 d. 選擇*更改密碼*。
更改群組（僅限本機用戶）	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。 c. 選擇“群組”標籤。 d. 或者，選擇群組名稱後的連結以在新瀏覽器標籤中查看群組的詳細資訊。 e. 選擇*編輯群組*來選擇不同的群組。 f. 選擇“儲存變更”。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇“群組”標籤。 c. 或者，選擇群組名稱後的連結以在新瀏覽器標籤中查看群組的詳細資訊。 d. 選擇*編輯群組*來選擇不同的群組。 e. 選擇“儲存變更”。

複製用戶

您可以複製現有使用者來建立具有相同權限的新使用者。

步驟

1. 選取使用者的複選框。
2. 選擇*動作* > 重複使用者。
3. 完成重複使用者嚮導。

刪除用戶

您可以刪除本機使用者以從系統中永久刪除該使用者。

您不能刪除 root 使用者。

步驟

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

使用單一登入 (SSO)

配置單一登入

啟用單一登入 (SSO) 後，只有使用貴組織實作的 SSO 登入流程授權使用者的憑證，使用者才能存取網格管理員、租用戶管理器、網格管理 API 或租用戶管理 API。本機使用者無法登入StorageGRID。

單一登入的工作原理

StorageGRID系統支援使用安全性斷言標記語言 2.0 (SAML 2.0) 標準的單一登入 (SSO)。

在啟用單一登入 (SSO) 之前，請先查看啟用 SSO 時StorageGRID登入和登出程序會受到怎樣的影響。

啟用 **SSO** 後**Sign in**

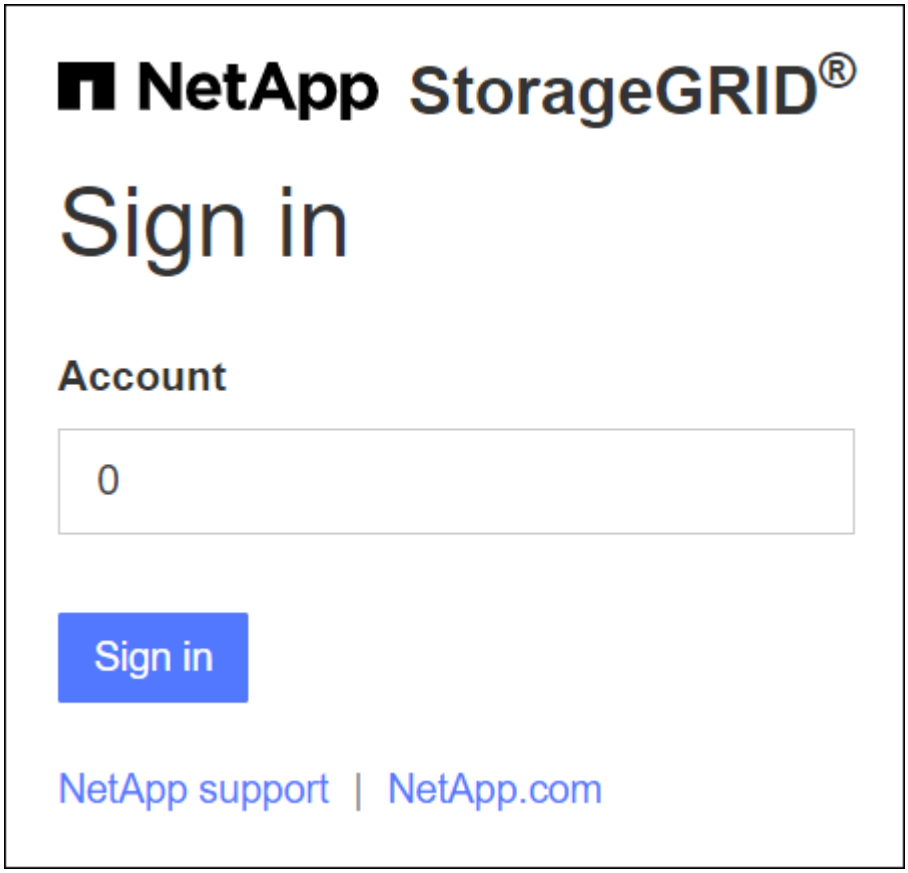
當啟用 SSO 並且您登入StorageGRID時，您將被重新導向到您組織的 SSO 頁面以驗證您的憑證。

步驟

1. 在 Web 瀏覽器中輸入任何StorageGRID管理節點的完全限定網域名稱或 IP 位址。

   出現StorageGRIDSign in頁面。

   - 如果這是您第一次在此瀏覽器上造訪該 URL，系統會提示您輸入帳戶 ID：

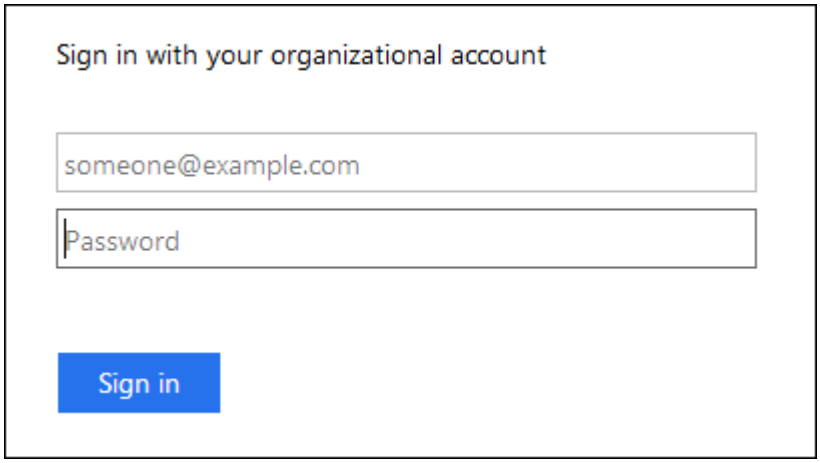


   - 如果您之前曾造訪過網格管理器或租用戶管理器，系統會提示您選擇最近的帳戶或輸入帳戶 ID：

當您Sign in租用戶帳戶的完整 URL（即完全限定網域名稱或 IP 位址，後面接著 `/?accountId=20-digit-account-id`）。相反，您會立即重定向到您組織的 SSO 登入頁面，您可以在其中使用您的 SSO 憑證登入。

2. 指示您是否要存取網格管理器或租戶管理器：
   - 若要存取網格管理器，請將「帳戶 **ID**」欄位留空，輸入「**0**」作為帳戶 ID，或選擇「網格管理員」（如果它出現在最近帳戶清單中）。
   - 若要存取租用戶管理器，請輸入 20 位租用戶帳號 ID，或按名稱選擇最近帳戶清單中出現的租用戶。
3. 選擇 **Sign in**

   StorageGRID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Sign in。

   如果您的 SSO 憑證正確：

a. 身分提供者 (IdP) 向StorageGRID提供驗證回應。

b. StorageGRID驗證身份驗證回應。

c. 如果回應有效且您屬於具有StorageGRID存取權限的聯合群組，您將登入網格管理器或租用戶管理器，具體取決於您選擇的帳戶。

> 如果服務帳戶無法訪問，您仍然可以登錄，只要您是屬於具有StorageGRID存取權限的聯合群組的現有使用者。

5. 或者，如果您有足夠的權限，可以存取其他管理節點，或存取網格管理器或租用戶管理器。

   您不需要重新輸入您的 SSO 憑證。

啟用 **SSO** 後退出

當為StorageGRID啟用 SSO 時，您登出時發生的情況取決於您登入的內容以及您從哪裡登出。

步驟

1. 找到使用者介面右上角的「退出」連結。
2. 選擇“退出”。

   出現StorageGRIDSign in頁面。 *最近的帳戶*下拉式選單已更新，包括*網格管理員*或租用戶的名稱，因此您將來可以更快地存取這些使用者介面。

如果您已登入...	然後您退出...	您已退出...
一個或多個管理節點上的網格管理器	任何管理節點上的網格管理器	所有管理節點上的網格管理器 *注意：*如果您使用 Azure 進行 SSO，可能需要幾分鐘才能退出所有管理節點。
一個或多個管理節點上的租戶管理器	任何管理節點上的租戶管理器	所有管理節點上的租戶管理器
網格管理器和租戶管理器	網格管理器	僅限網格管理器。您也必須退出租戶管理器才能退出 SSO。

> 表格總結了當您使用單一瀏覽器工作階段時登出時發生的情況。如果您透過多個瀏覽器會話登入StorageGRID ，則必須分別登出所有瀏覽器工作階段。

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，請查看要求和注意事項。

身份提供者要求

StorageGRID支援以下 SSO 身分提供者 (IdP)：

- Active Directory 聯合驗證服務 (AD FS)
- Azure Active Directory (Azure AD)
- Ping聯邦

您必須先為StorageGRID系統設定身分聯合，然後才能設定 SSO 身分提供者。用於身分聯合的 LDAP 服務類型控制您可以實現哪種類型的 SSO。

配置的 **LDAP** 服務類型	**SSO** 身分提供者的選項
活動目錄	• 活動目錄 • Azure • Ping聯邦
Azure	Azure

AD FS 要求

您可以使用下列任一版本的 AD FS：

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

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

其他要求

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

Azure 的注意事項

如果您使用 Azure 作為 SSO 類型，且使用者的使用者主體名稱不使用 sAMAccountName 作為前綴，則當StorageGRID與 LDAP 伺服器失去連線時，可能會發生登入問題。若要允許使用者登入，您必須恢復與 LDAP 伺服器的連線。

伺服器證書要求

預設情況下， StorageGRID在每個管理節點上使用管理介面憑證來保護對網格管理器、租用戶管理員、網格管理 API 和租用戶管理 API 的存取。為StorageGRID設定信賴方信任 (AD FS)、企業應用程式 (Azure) 或服務供應商連線 (PingFederate) 時，您可以使用伺服器憑證作為StorageGRID請求的簽章憑證。

如果你還沒有"為管理介面配置自訂證書"，你現在就應該這麼做。當您安裝自訂伺服器憑證時，它將用於所有管理節點，並且您可以在所有StorageGRID依賴方信任、企業應用程式或SP連線中使用它。

不建議在依賴方信任、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且您恢復了它，則會產生新的預設伺服器憑證。在登入復原的節點之前，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。

您可以透過登入節點的命令 shell 並轉到 `/var/local/mgmt-api`目錄。自訂伺服器憑證名為 `custom-server.crt`。該節點的預設伺服器憑證名為 `server.crt`。

端口要求

受限的網格管理器或租戶管理器連接埠上不提供單一登入 (SSO)。如果您希望使用者透過單一登入進行驗證，則必須使用預設 HTTPS 連接埠 (443)。看"控制外部防火牆的訪問" 。

確認聯合用戶可以登入

在啟用單一登入 (SSO) 之前，您必須確認至少有一個共同使用者可以登入網格管理員和任何現有租用戶帳戶的租用戶管理員。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您已經配置了身份聯合。

步驟

1. 如果存在現有租用戶帳戶，請確認沒有任何租戶使用其自己的身分來源。

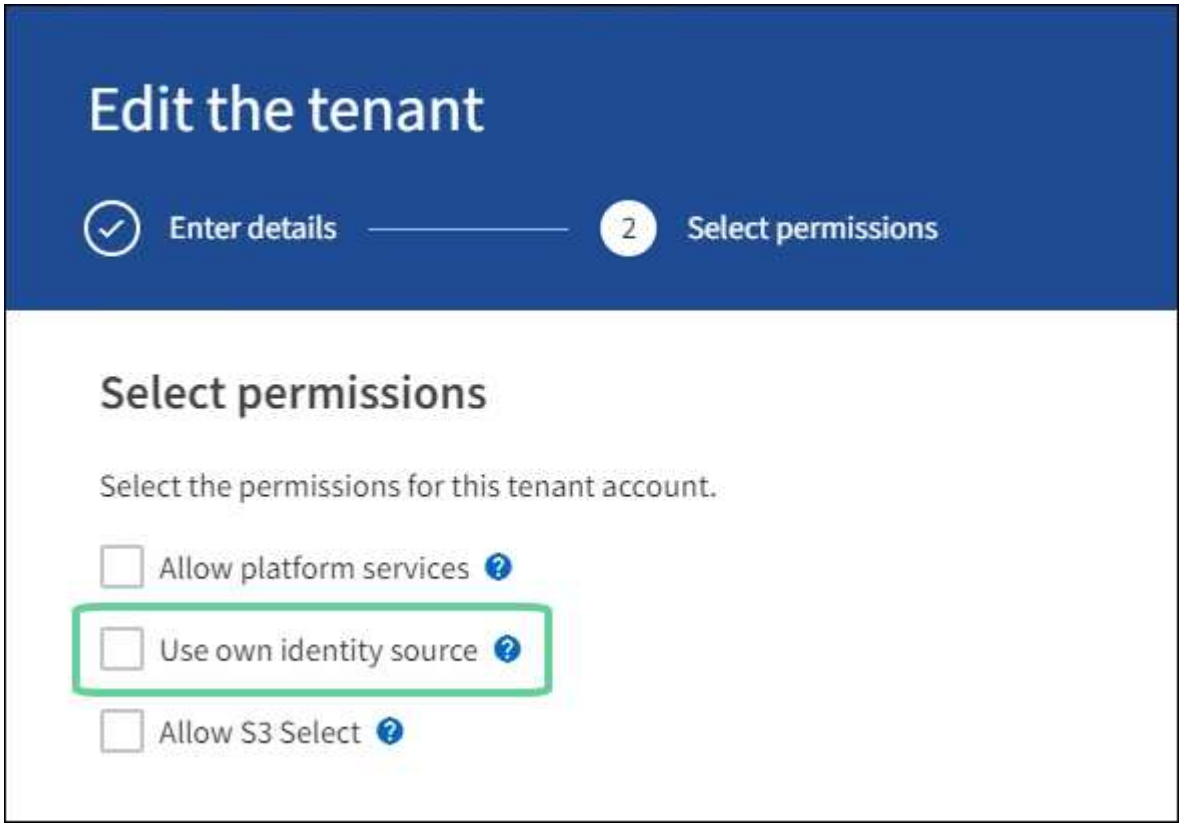
   啟用 SSO 時，租用戶管理員中設定的身份來源將會被網格管理器中設定的身份來源覆寫。屬於租用戶身分來源的使用者將無法再登入，除非他們擁有 Grid Manager 身分來源的帳戶。

   a. Sign in每個租用戶帳戶的租用戶管理員。
   b. 選擇*存取管理* > 身分聯合。
   c. 確認未選取「啟用身份聯合」複選框。
   d. 如果是，請確認該租用戶帳戶可能使用的任何聯合群組不再需要，清除複選框，然後選擇*儲存*。

2. 確認聯合用戶可以存取網格管理器：
   a. 從網格管理員中，選擇 配置 > 存取控制 > 管理群組。
   b. 確保已從 Active Directory 身分來源匯入至少一個聯合群組，並且已為其指派 Root 存取權限。
   c. 登出。
   d. 確認您可以作為聯合群組中的使用者重新登入網格管理器。

3. 如果存在現有的租用戶帳戶，請確認具有 Root 存取權限的共同使用者可以登入：
   a. 從網格管理器中選擇*TENANTS*。
   b. 選擇租用戶帳戶，然後選擇*操作* > 編輯。
   c. 在「輸入詳細資料」標籤上，選擇「繼續」。

d. 如果選取了*使用自己的身分來源*複選框，請取消選取該框並選擇*儲存*。



出現「租戶」頁面。

a. 選擇租戶帳號，選擇*Sign in*，以本地root用戶登入租戶帳號。

b. 從租用戶管理員中，選擇*存取管理* > 群組。

c. 確保網格管理員中的至少一個聯合群組已指派此租用戶的 Root 存取權限。

d. 登出。

e. 確認您可以以聯合群組中的使用者重新登入租用戶。

相關資訊

- "單一登入的要求和注意事項"
- "管理管理員群組"
- "使用租用戶帳戶"

使用沙盒模式

您可以使用沙盒模式來設定和測試單一登入 (SSO)，然後為所有StorageGRID使用者啟用它。啟用 SSO 後，您可以在需要變更或重新測試設定時返回沙盒模式。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

- 您已為StorageGRID系統配置身份聯合。
- 對於身分識別聯合 **LDAP** 服務類型，您可以根據計畫使用的 SSO 身分提供者選擇 Active Directory 或 Azure。

配置的 **LDAP** 服務類型	**SSO** 身分提供者的選項
活動目錄	• 活動目錄 • Azure • Ping聯邦
Azure	Azure

關於此任務

當啟用 SSO 且使用者嘗試登入管理節點時， StorageGRID會向 SSO 身分提供者傳送驗證請求。反過來，SSO 身份提供者將身份驗證回應傳送回StorageGRID，指示身份驗證請求是否成功。對於成功的請求：

- Active Directory 或 PingFederate 的回應包括使用者的通用唯一識別碼 (UUID)。
- Azure 的回應包括使用者主體名稱 (UPN)。

為了允許StorageGRID （服務提供者）和 SSO 身分提供者就使用者驗證請求進行安全通信，您必須在StorageGRID中設定某些設定。接下來，您必須使用 SSO 身分提供者的軟體為每個管理節點建立信賴方信任 (AD FS)、企業應用程式 (Azure) 或服務提供者 (PingFederate)。最後，您必須返回StorageGRID以啟用 SSO。

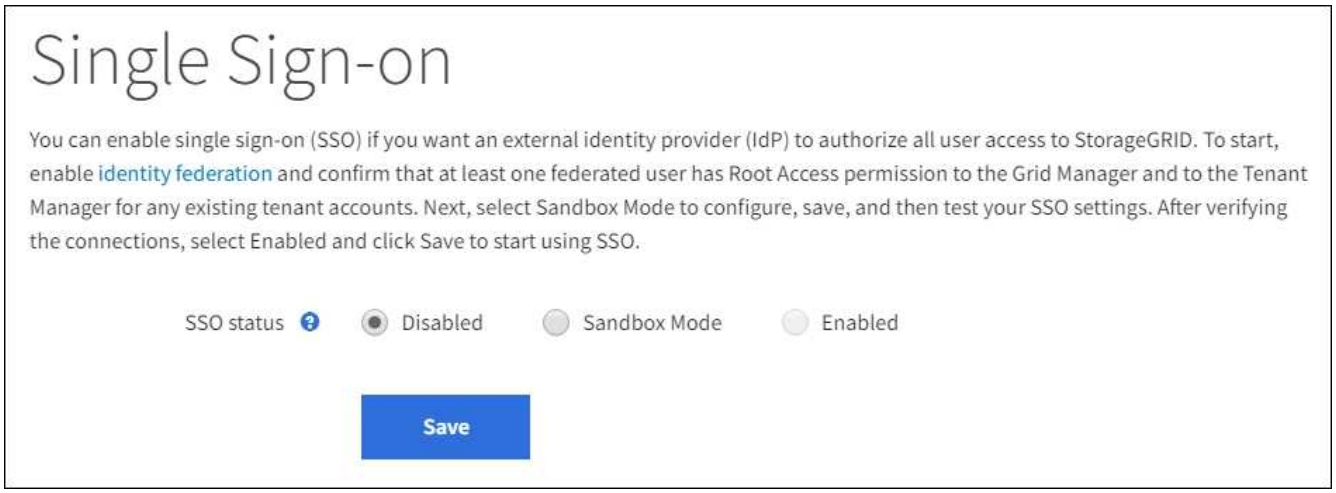
沙盒模式可以輕鬆執行此來回配置，並在啟用 SSO 之前測試所有設定。當您使用沙盒模式時，使用者無法使用 SSO 登入。

訪問沙盒模式

步驟

1. 選擇*設定* > 存取控制 > 單一登入。

   出現「單一登入」頁面，其中選擇了「已停用」選項。



如果未出現 SSO 狀態選項，請確認您已將身分提供者設定為聯合身分識別來源。看"單一登入的要求和注意事項" 。

2. 選擇*沙盒模式*。

   出現身分提供者部分。

輸入身份提供者詳細信息

步驟

1. 從下拉清單中選擇 **SSO** 類型。
2. 根據您選擇的 SSO 類型填入身分提供者部分中的欄位。

活動目錄

a. 輸入身分識別提供者的*聯合身分驗證服務名稱*，與其在 Active Directory 聯合驗證服務 (AD FS) 中顯示的名稱完全一致。

> 若要找到聯合服務名稱，請前往 Windows 伺服器管理員。選擇“工具”>“AD FS 管理”。從操作選單中，選擇*編輯聯合服務屬性*。聯合服務名稱顯示在第二個欄位中。

b. 指定當身分識別提供者回應StorageGRID請求傳送 SSO 設定資訊時將使用哪個 TLS 憑證來保護連線。

- 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 CA 憑證來保護連線。
- 使用自訂 **CA** 憑證：使用自訂 CA 憑證來保護連線。

  如果選擇此設置，請複製自訂憑證的文字並將其貼上到 **CA** 憑證 文字方塊中。
- 不要使用 **TLS**：不要使用 TLS 憑證來保護連線。

> 如果您更改了 CA 證書，請立即"在管理節點上重新啟動 mgmt-api 服務"並測試是否成功 SSO 進入網格管理器。

c. 在「依賴方」部分中，指定StorageGRID的「依賴方識別碼」。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管理節點，且您不打算在將來新增更多管理節點，請輸入 `SG`或者 `StorageGRID`。
- 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]`在標識符中。例如， `SG-[HOSTNAME]`。這將產生一個表，根據節點的主機名稱顯示系統中每個管理節點的依賴方識別碼。

> 您必須為StorageGRID系統中的每個管理節點建立一個依賴方信任。每個管理節點都擁有依賴方信任，確保使用者可以安全地登入和登出任何管理節點。

d. 選擇*儲存*。

*儲存*按鈕上會出現綠色複選標記，持續幾秒鐘。

Azure

a. 指定當身分識別提供者回應StorageGRID請求傳送 SSO 設定資訊時將使用哪個 TLS 憑證來保護連線。

- 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 CA 憑證來保護連線。
- 使用自訂 **CA** 憑證：使用自訂 CA 憑證來保護連線。

  如果選擇此設置，請複製自訂憑證的文字並將其貼上到 **CA** 憑證 文字方塊中。

- 不要使用 **TLS**：不要使用 TLS 憑證來保護連線。

> 如果您更改了 CA 證書，請立即"在管理節點上重新啟動 mgmt-api 服務"並測試是否成功 SSO 進入網格管理器。

b. 在企業應用程式部分，指定StorageGRID的 企業應用程式名稱。此值控制您在 Azure AD 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管理節點，且您不打算在將來新增更多管理節點，請輸入 `SG`或者 `StorageGRID`。
- 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]`在標識符中。例如， `SG-[HOSTNAME]` 。這將產生一個表，根據節點的主機名稱顯示系統中每個管理節點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。每個管理節點都有一個企業應用程序，可確保使用者可以安全地登入和登出任何管理節點。

c. 請依照以下步驟操作"在 Azure AD 中建立企業應用程式"為表中列出的每個管理節點建立一個企業應用程式。

d. 從 Azure AD 複製每個企業應用程式的聯合元資料 URL。然後，將此 URL 貼到StorageGRID中對應的 **Federation metadata URL** 欄位中。

e. 複製並貼上所有管理節點的聯合元資料 URL 後，選擇 儲存。

*儲存*按鈕上會出現綠色複選標記，持續幾秒鐘。

Ping聯邦

a. 指定當身分識別提供者回應StorageGRID請求傳送 SSO 設定資訊時將使用哪個 TLS 憑證來保護連線。

- 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 CA 憑證來保護連線。
- 使用自訂 **CA** 憑證：使用自訂 CA 憑證來保護連線。

  如果選擇此設置，請複製自訂憑證的文字並將其貼上到 **CA** 憑證 文字方塊中。

- 不要使用 **TLS**：不要使用 TLS 憑證來保護連線。

> 如果您更改了 CA 證書，請立即"在管理節點上重新啟動 mgmt-api 服務"並測試是否成功 SSO 進入網格管理器。

b. 在服務提供者 (SP) 部分中，指定StorageGRID的 * SP連線 ID *。此值控制您在 PingFederate 中為每個SP連線使用的名稱。

- 例如，如果您的網格只有一個管理節點，且您不打算在將來新增更多管理節點，請輸入 `SG`或者 `StorageGRID`。

- 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]`在標識符中。例如， `SG-[HOSTNAME]` 。這將產生一個表，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。每個管理節點都有一個SP連接，可確保使用者可以安全地登入和登出任何管理節點。

c. 在 **Federation metadata URL** 欄位中指定每個管理節點的聯合元資料 URL。

使用以下格式：

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

d. 選擇*儲存*。

*儲存*按鈕上會出現綠色複選標記，持續幾秒鐘。

配置信賴方信任、企業應用程式或**SP**連接

儲存配置後，會出現沙盒模式確認通知。此通知確認沙盒模式現已啟用並提供概述說明。

StorageGRID可依需求維持沙盒模式。但是，當在單一登入頁面上選擇「沙盒模式」時，所有StorageGRID使用者的 SSO 都會被停用。只有本地用戶可以登入。

請依照下列步驟設定信賴方信任（Active Directory）、完成企業應用程式（Azure）或設定SP連線（PingFederate）。

活動目錄

步驟

1. 前往 Active Directory 聯合驗證服務 (AD FS)。
2. 使用StorageGRID單一登入頁面上的表格中顯示的每個依賴方標識符，為StorageGRID建立一個或多個依賴方信任。

   您必須為表中顯示的每個管理節點建立一個信任。

   有關說明，請訪問"在 AD FS 中創造信賴方信任"。

Azure

步驟

1. 從您目前登入的管理節點的單一登入頁面，選擇按鈕下載並儲存 SAML 元資料。
2. 然後，對於網格中的任何其他管理節點，重複以下步驟：
   a. Sign in節點。
   b. 選擇*設定* > 存取控制 > 單一登入。
   c. 下載並儲存該節點的 SAML 元資料。
3. 前往 Azure 入口網站。
4. 請依照以下步驟操作"在 Azure AD 中建立企業應用程式"將每個管理節點的 SAML 元資料檔案上傳到其對應的 Azure 企業應用程式中。

Ping聯邦

步驟

1. 從您目前登入的管理節點的單一登入頁面，選擇按鈕下載並儲存 SAML 元資料。
2. 然後，對於網格中的任何其他管理節點，重複以下步驟：
   a. Sign in節點。
   b. 選擇*設定* > 存取控制 > 單一登入。
   c. 下載並儲存該節點的 SAML 元資料。
3. 前往 PingFederate。
4. "為StorageGRID建立一個或多個服務提供者（SP）連接" 。使用每個管理節點的SP連線 ID（顯示在StorageGRID單一登入頁面上的表格中）以及為該管理節點下載的 SAML 元資料。

   您必須為表格中顯示的每個管理節點建立一個SP連線。

測試 **SSO** 連接

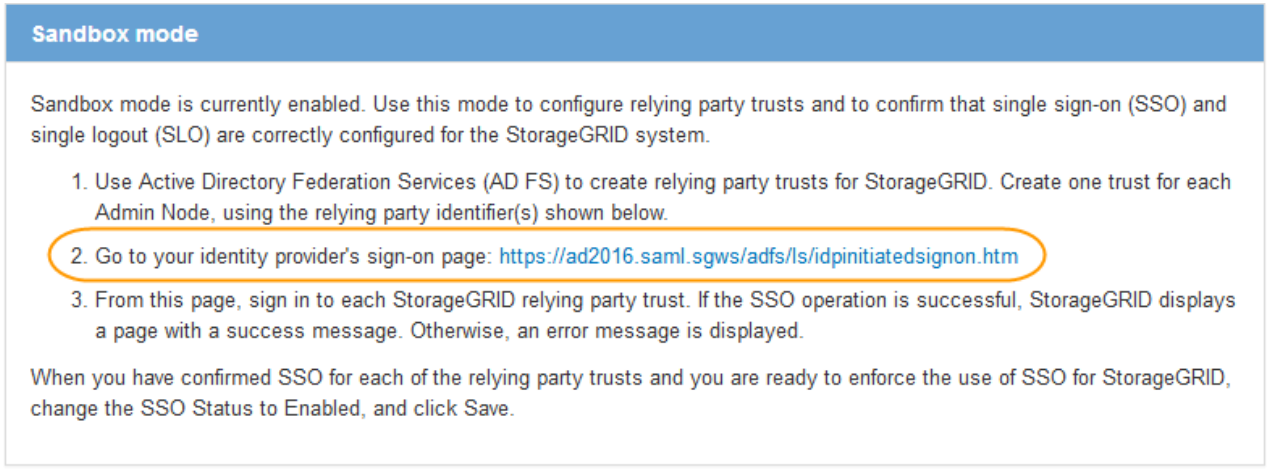
在強制整個StorageGRID系統使用單一登入之前，您應該確認每個管理節點的單一登入和單一登出都已正確配置。

活動目錄

步驟

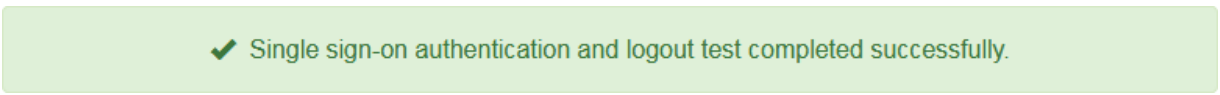
1. 在StorageGRID單一登入頁面中，找到沙盒模式訊息中的連結。

   該 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，以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，請選擇 **Sign in**下列網站之一，選擇主管理節點的信賴方標識符，然後選擇 **Sign in**。

4. 輸入您的聯合用戶名和密碼。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。



   - 如果 SSO 操作不成功，則會顯示錯誤訊息。解決問題，清除瀏覽器的 cookie，然後重試。
5. 重複這些步驟來驗證網格中每個管理節點的 SSO 連線。

Azure

步驟

1. 前往 Azure 入口網站中的單一登入頁面。
2. 選擇*測試此應用程式*。
3. 輸入聯合用戶的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。

     ✔ Single sign-on authentication and logout test completed successfully.

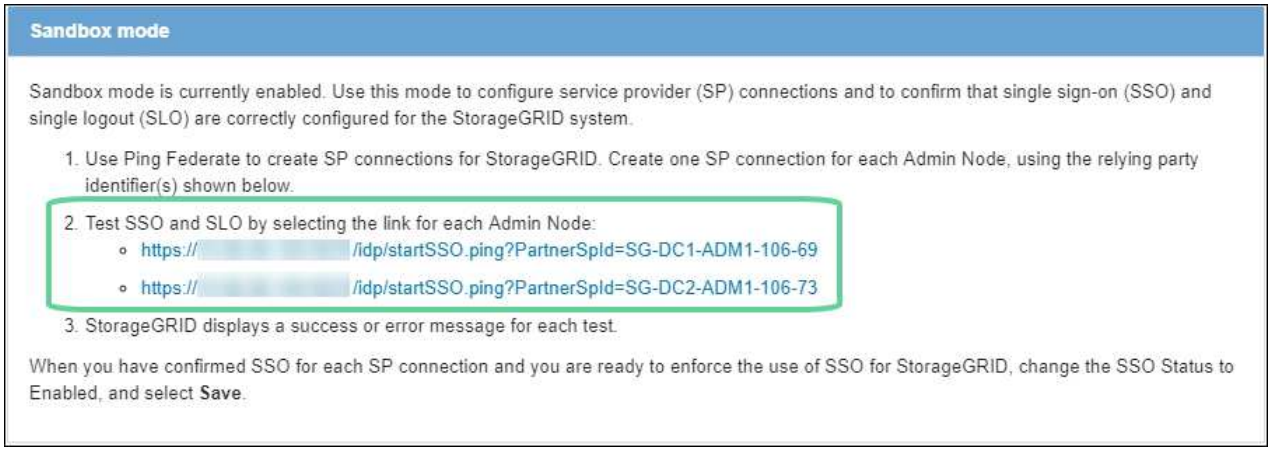
   - 如果 SSO 操作不成功，則會顯示錯誤訊息。解決問題，清除瀏覽器的 cookie，然後重試。
4. 重複這些步驟來驗證網格中每個管理節點的 SSO 連線。

Ping聯邦

步驟

1. 從StorageGRID單一登入頁面，選擇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. 輸入聯合用戶的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。

     ✔ Single sign-on authentication and logout test completed successfully.

   - 如果 SSO 操作不成功，則會顯示錯誤訊息。解決問題，清除瀏覽器的 cookie，然後重試。
3. 選擇下一個連結來驗證網格中每個管理節點的 SSO 連線。

   如果您看到「頁面已過期」訊息，請選擇瀏覽器中的「返回」按鈕並重新提交您的憑證。

啟用單一登入

當您確認可以使用 SSO 登入每個管理節點後，您可以為整個StorageGRID系統啟用 SSO。

啟用 SSO 後，所有使用者都必須使用 SSO 來存取網格管理器、租用戶管理器、網格管理 API 和租用戶管理 API。本機用戶無法再存取StorageGRID。

步驟

1. 選擇*設定* > 存取控制 > 單一登入。
2. 將 SSO 狀態變更為 已啟用。
3. 選擇*儲存*。
4. 查看警告訊息，然後選擇“確定”。

   單一登入現已啟用。

如果您使用 Azure 入口網站並從用於存取 Azure 的相同電腦存取StorageGRID ，請確保 Azure 入口網站使用者也是授權的StorageGRID使用者（已匯入StorageGRID 的聯合群組中的使用者）或在嘗試登入StorageGRID之前登出 Azure 入口網站。

在 **AD FS** 中創造信賴方信任

您必須使用 Active Directory 聯合驗證服務 (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 指令、透過從StorageGRID匯入 SAML 元資料或手動輸入資料來建立信賴方信任。

開始之前

- 您已為StorageGRID設定單一登入，並選擇 **AD FS** 作為 SSO 類型。
- 在網格管理員的單一登入頁面上選擇了*沙盒模式*。看"使用沙盒模式" 。
- 您知道系統中每個管理節點的完全限定網域名稱（或 IP 位址）和信賴方識別碼。您可以在StorageGRID單一登入頁面上的管理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一個依賴方信任。每個管理節點都擁有依賴方信任，確保使用者可以安全地登入和登出任何管理節點。

- 您具有在 AD FS 中建立信任方信任的經驗，或者您可以存取 Microsoft AD FS 文件。
- 您正在使用 AD FS 管理管理單元，並且您屬於管理員群組。
- 如果您手動建立依賴方信任，則您擁有為StorageGRID管理介面上傳的自訂證書，或者您知道如何從命令 shell 登入管理節點。

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，您會注意到過程中略有不同。如果您有任何疑問，請參閱 Microsoft AD FS 文件。

使用 **Windows PowerShell** 建立信賴方信任

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，右鍵單擊選擇 PowerShell 圖標，然後選擇*以管理員身份執行*。
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"
   ```

   - 為了 *Admin_Node_Identifier*，輸入管理節點的依賴方標識符，與單一登入頁面上顯示的完全一致。例如， `SG-DC1-ADM1` 。
   - 為了 *Admin_Node_FQDN*，輸入同一管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。）
3. 從 Windows 伺服器管理員中，選擇「工具」>「AD FS 管理」。

   出現 AD FS 管理工具。
4. 選擇 **AD FS** > 依賴方信任。

   出現依賴方信任的清單。
5. 在新建立的依賴方信任中新增存取控制策略：
   a. 找到您剛剛創建的信任方信任。
   b. 右鍵單擊信任，然後選擇“編輯存取控制策略”。
   c. 選擇存取控制策略。
   d. 選擇“應用”，然後選擇“確定”
6. 在新建立的依賴方信任中新增聲明發布策略：
   a. 找到您剛剛創建的信任方信任。
   b. 右鍵點選信託，然後選擇「編輯索賠頒發政策」。
   c. 選擇*新增規則*。
   d. 在選擇規則範本頁面上，從清單中選擇*將 LDAP 屬性傳送為聲明*，然後選擇*下一步*。
   e. 在設定規則頁面上，輸入此規則的顯示名稱。

      例如，**ObjectGUID** 到名稱 **ID** 或 **UPN** 到名稱 **ID**。
   f. 對於屬性存儲，選擇*Active Directory*。
   g. 在映射表的 LDAP 屬性列中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   h. 在映射表的傳出聲明類型列中，從下拉清單中選擇*名稱 ID*。
   i. 選擇“完成”，然後選擇“確定”。
7. 確認元資料已成功導入。
   a. 右鍵單擊信賴方信任以開啟其屬性。
   b. 確認「**Endpoints**」、「**Identifiers**」和「**Signature**」標籤上的欄位已填入。

      如果缺少元數據，請確認聯邦元數據地址是否正確，或手動輸入值。

8. 重複這些步驟，為StorageGRID系統中的所有管理節點配置依賴方信任。
9. 完成後，返回StorageGRID並測試所有依賴方信任以確認它們配置正確。看"使用沙盒模式"以取得說明。

透過匯入聯合元資料創建信賴方信任

您可以透過存取每個管理節點的 SAML 元資料來匯入每個依賴方信任的值。

步驟

1. 在 Windows 伺服器管理員中，選擇“工具”，然後選擇“AD FS 管理”。
2. 在操作下，選擇*新增依賴方信任*。
3. 在歡迎頁面上，選擇*索賠意識*，然後選擇*開始*。
4. 選擇*匯入線上或本機網路上發佈的有關依賴方的資料*。
5. 在 聯合元資料位址（主機名稱或 **URL**） 中，鍵入此管理節點的 SAML 元資料的位置：

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

   為了 `Admin_Node_FQDN`，輸入同一管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。 ）

6. 完成依賴方信任嚮導，儲存依賴方信任，然後關閉嚮導。

   輸入顯示名稱時，請使用管理節點的依賴方標識符，與網格管理器中的單點登入頁面上顯示的完全一樣。例如， `SG-DC1-ADM1` 。

7. 新增聲明規則：
   a. 右鍵點選信託，然後選擇「編輯索賠頒發政策」。
   b. 選擇*新增規則*：
   c. 在選擇規則範本頁面上，從清單中選擇*將 LDAP 屬性傳送為聲明*，然後選擇*下一步*。
   d. 在設定規則頁面上，輸入此規則的顯示名稱。

      例如，**ObjectGUID** 到名稱 **ID** 或 **UPN** 到名稱 **ID**。

   e. 對於屬性存儲，選擇*Active Directory*。
   f. 在映射表的 LDAP 屬性列中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   g. 在映射表的傳出聲明類型列中，從下拉清單中選擇*名稱 ID*。
   h. 選擇“完成”，然後選擇“確定”。
8. 確認元資料已成功導入。
   a. 右鍵單擊信賴方信任以開啟其屬性。
   b. 確認「**Endpoints**」、「**Identifiers**」和「**Signature**」標籤上的欄位已填入。

      如果缺少元數據，請確認聯邦元數據地址是否正確，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配置依賴方信任。
10. 完成後，返回StorageGRID並測試所有依賴方信任以確認它們配置正確。看"使用沙盒模式"以取得說明。

手動創建信賴方信任

如果您選擇不匯入依賴部分信託的數據，您可以手動輸入值。

步驟

1. 在 Windows 伺服器管理員中，選擇“工具”，然後選擇“AD FS 管理”。
2. 在操作下，選擇*新增依賴方信任*。
3. 在歡迎頁面上，選擇*索賠意識*，然後選擇*開始*。
4. 選擇*手動輸入依賴方的資料*，然後選擇*下一步*。
5. 完成依賴方信任嚮導：
   a. 輸入此管理節點的顯示名稱。

      為了保持一致性，請使用管理節點的依賴方標識符，與網格管理器中的單點登入頁面上顯示的完全一樣。例如， `SG-DC1-ADM1` 。

   b. 跳過配置可選令牌加密憑證的步驟。
   c. 在設定 URL 頁面上，選取 啟用對 **SAML 2.0 WebSSO** 協定的支援 複選框。
   d. 輸入管理節點的 SAML 服務端點 URL：

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

      為了 `*Admin_Node_FQDN*`中，輸入管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。 ）

   e. 在設定標識符頁面上，為同一個管理節點指定依賴方識別碼：

      `*Admin_Node_Identifier*`

      為了 `*Admin_Node_Identifier*`，輸入管理節點的依賴方標識符，與單一登入頁面上顯示的完全一致。例如， `SG-DC1-ADM1` 。

   f. 檢查設置，儲存信賴方信任，然後關閉精靈。

      出現「編輯索賠簽發政策」對話框。

      如果未出現對話框，請右鍵點選信任，然後選擇「編輯聲明頒發政策」。

6. 若要啟動聲明規則精靈，請選擇*新增規則*：
   a. 在選擇規則範本頁面上，從清單中選擇*將 LDAP 屬性傳送為聲明*，然後選擇*下一步*。
   b. 在設定規則頁面上，輸入此規則的顯示名稱。

      例如，**ObjectGUID** 到名稱 **ID** 或 **UPN** 到名稱 **ID**。

c. 對於屬性存儲，選擇*Active Directory*。

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

e. 在映射表的傳出聲明類型列中，從下拉清單中選擇*名稱 ID*。

f. 選擇“完成”，然後選擇“確定”。

7. 右鍵單擊信賴方信任以開啟其屬性。

8. 在「端點」標籤上，設定單點登出 (SLO) 的端點：

a. 選擇“新增 SAML”。

b. 選擇*端點類型* > **SAML** 登出。

c. 選擇*綁定* > 重定向。

d. 在「可信任 **URL**」欄位中，輸入用於從此管理節點單點登出 (SLO) 的 URL：

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

為了 `*Admin_Node_FQDN*`中，輸入管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。）

a. 選擇“確定”。

9. 在「簽署」標籤上，指定此信賴方信任的簽章憑證：

a. 新增自訂憑證：

- 如果您有上傳到StorageGRID 的自訂管理證書，請選擇該證書。
- 如果您沒有自訂證書，請登入管理節點，前往 `/var/local/mgmt-api`管理節點的目錄，並且加入 `custom-server.crt`證書文件。

> ⓘ 使用管理節點的預設證書(`server.crt`) 是不推薦的。如果管理節點發生故障，則恢復節點時將重新產生預設證書，並且您需要更新信賴方信任。

b. 選擇“應用”，然後選擇“確定”。

依賴方屬性已儲存並關閉。

10. 重複這些步驟，為StorageGRID系統中的所有管理節點配置依賴方信任。

11. 完成後，返回StorageGRID並測試所有依賴方信任以確認它們配置正確。看"使用沙盒模式"以取得說明。

在 **Azure AD** 中建立企業應用程式

您使用 Azure AD 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設定單一登錄，並選擇 **Azure** 作為 SSO 類型。
- 在網格管理員的單一登入頁面上選擇了*沙盒模式*。看"使用沙盒模式" 。
- 您的系統中的每個管理節點都有*企業應用程式名稱*。您可以從StorageGRID單一登入頁面上的管理節點詳

細資料表中複製這些值。

> 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。每個管理節點都有一個企業應用程序，可確保使用者可以安全地登入和登出任何管理節點。

- 您有在 Azure Active Directory 中建立企業應用程式的經驗。
- 您有一個具有有效訂閱的 Azure 帳戶。
- 您在 Azure 帳戶中擁有下列角色之一：全域管理員、雲端應用程式管理員、應用程式管理員或服務主體的擁有者。

存取 **Azure AD**

步驟

1. 登入 "Azure 入口網站"。
2. 導航至 "Azure Active Directory"。
3. 選擇 "企業應用程式"。

建立企業應用程式並儲存**StorageGRID SSO** 配置

若要在StorageGRID中儲存 Azure 的 SSO 配置，您必須使用 Azure 為每個管理節點建立一個企業應用程式。您將從 Azure 複製聯合元資料 URL，並將其貼上到StorageGRID單一登入頁面上對應的 聯合元資料 **URL** 欄位中。

步驟

1. 對每個管理節點重複以下步驟。
   a. 在 Azure Enterprise 應用程式窗格中，選擇「新應用程式」。
   b. 選擇*創建您自己的應用程式*。
   c. 對於名稱，請輸入從StorageGRID單一登入頁面上的管理節點詳細資料表複製的 企業應用程式名稱。
   d. 保持選取*整合您在圖庫中找不到的任何其他應用程式（非圖庫）*單選按鈕。
   e. 選擇“創建”。
   f. 選擇*2 中的*開始*連結。設定單一登入*框，或選擇左邊距中的*單一登入*連結。
   g. 選擇 **SAML** 框。
   h. 複製 **App Federation Metadata Url**，您可以在 **Step 3 SAML Signing Certificate** 下找到它。
   i. 前往StorageGRID單一登入頁面，並將 URL 貼到與您使用的 企業應用程式名稱 相對應的 聯合元資料 **URL** 欄位中。
2. 為每個管理節點貼上聯合元資料 URL 並對 SSO 配置進行所有其他必要的變更後，在StorageGRID單一登入頁面上選擇 儲存。

下載每個管理節點的 **SAML** 元數據

儲存 SSO 設定後，您可以為StorageGRID系統中的每個管理節點下載一個 SAML 元資料檔。

步驟

1. 對每個管理節點重複這些步驟。
   a. 從管理節點Sign inStorageGRID 。
   b. 選擇*設定* > 存取控制 > 單一登入。
   c. 選擇按鈕下載該管理節點的 SAML 元資料。
   d. 儲存文件，然後將其上傳到 Azure AD。

將 **SAML** 元資料上傳到每個企業應用程式

為每個StorageGRID管理節點下載 SAML 元資料檔案後，在 Azure AD 中執行下列步驟：

步驟

1. 返回 Azure 入口網站。
2. 對每個企業應用程式重複以下步驟：

   > 您可能需要刷新企業應用程式頁面才能看到先前在清單中新增的應用程式。

   a. 轉到企業應用程式的屬性頁面。
   b. 將 需要分配 設定為 否（除非您想單獨配置分配）。
   c. 前往單一登入頁面。
   d. 完成 SAML 設定。
   e. 選擇*上傳元資料檔案*按鈕，然後選擇您為對應管理節點下載的 SAML 元資料檔案。
   f. 檔案載入後，選擇*儲存*，然後選擇*X*關閉窗格。您將返回使用 SAML 設定單一登入頁面。
3. 請依照以下步驟操作"使用沙盒模式"測試每個應用程式。

在 **PingFederate** 中建立服務提供者 **(SP)** 連接

您使用 PingFederate 為系統中的每個管理節點建立服務提供者 (SP) 連線。為了加快這個過程，您將從StorageGRID匯入 SAML 元資料。

開始之前

- 您已為StorageGRID設定單一登錄，並選擇 **Ping Federate** 作為 SSO 類型。
- 在網格管理員的單一登入頁面上選擇了*沙盒模式*。看"使用沙盒模式" 。
- 您系統中每個管理節點都有* SP連線 ID *。您可以在StorageGRID單一登入頁面上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** 元資料。
- 您有在 PingFederate 伺服器中建立SP連線的經驗。
- 你有https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["管理員參考指南"^]用於 PingFederate 伺服器。PingFederate 文件提供了詳細的逐步說明和解釋。
- 你有"管理員權限"用於 PingFederate 伺服器。

關於此任務

這些說明總結如何將 PingFederate Server 版本 10.3 設定為StorageGRID的 SSO 提供者。如果您使用的是其他版本的 PingFederate，則可能需要調整這些說明。有關您的版本的詳細說明，請參閱 PingFederate 伺服器文件。

完成 **PingFederate** 中的先決條件

在建立將用於StorageGRID 的SP連線之前，您必須完成 PingFederate 中的先決條件任務。配置SP連線時，您將使用這些先決條件中的資訊。

建立資料儲存

如果您還沒有，請建立資料儲存以將 PingFederate 連接到 AD FS LDAP 伺服器。使用您使用過的值"配置身份聯合"在StorageGRID中。

- 類型：目錄（LDAP）
- **LDAP** 類型：Active Directory
- 二進位屬性名稱：在 LDAP 二進位屬性標籤上輸入 **objectGUID**，與所示完全一致。

建立密碼憑證驗證器

如果您還沒有，請建立密碼憑證驗證器。

- 類型：LDAP 使用者名稱密碼憑證驗證器
- 資料儲存：選擇您建立的資料儲存。
- 搜尋基礎：輸入來自 LDAP 的資訊（例如，DC=saml,DC=sgws）。
- 搜尋篩選器：sAMAccountName=${username}
- 範圍：子樹

建立 **IdP** 適配器實例

如果您還沒有，請建立 IdP 適配器實例。

步驟

1. 前往*身份驗證* > 整合 > **IdP** 適配器。
2. 選擇“建立新實例”。
3. 在類型標籤上，選擇*HTML 表單 IdP 適配器*。
4. 在 IdP 適配器標籤上，選擇*為「憑證驗證器」新增一行*。
5. 選擇密碼憑證驗證器你創造的。
6. 在適配器屬性標籤上，選擇 **Pseudonym** 的 **username** 屬性。
7. 選擇*儲存*。

建立或匯入簽章憑證

如果您還沒有，請建立或匯入簽名證書。

步驟

1. 前往*安全* > 簽署和解密金鑰和憑證。
2. 建立或匯入簽名證書。

在 **PingFederate** 中建立**SP**連接

在 PingFederate 中建立SP連線時，您會匯入從StorageGRID為管理節點下載的 SAML 元資料。元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連接，以便使用者可以安全地登入和登出任何節點。使用這些說明來建立第一個SP連線。然後，轉到建立其他SP連接建立您需要的任何其他連線。

選擇**SP**連線類型

步驟

1. 前往*應用程式* > 整合 > * SP連接*。
2. 選擇*建立連線*。
3. 選擇*不要對此連線使用範本*。
4. 選擇 瀏覽器 **SSO** 設定檔 和 **SAML 2.0** 作為協定。

導入**SP**元數據

步驟

1. 在導入元資料標籤上，選擇*檔案*。
2. 選擇從管理節點的StorageGRID單一登入頁面下載的 SAML 元資料檔。
3. 查看元資料摘要和常規資訊標籤上提供的資訊。

   合作夥伴的實體 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。

4. 選擇“下一步”。

設定 **IdP** 瀏覽器 **SSO**

步驟

1. 從瀏覽器 SSO 標籤中，選擇 設定瀏覽器 **SSO**。
2. 在 SAML 設定檔標籤上，選擇 * SP-initiated SSO*、* SP-initial SLO*、* IdP-initiated SSO* 和 * IdP-initiated SLO* 選項。
3. 選擇“下一步”。
4. 在「斷言生命週期」標籤上，不做任何更改。
5. 在「斷言建立」標籤上，選擇「配置斷言建立」。
   a. 在「身分映射」標籤上，選擇「標準」。
   b. 在屬性合約標籤上，使用 **SAML_SUBJECT** 作為屬性合約和匯入的未指定的名稱格式。

6. 對於延長合同，選擇“刪除”以刪除 `urn:oid`，未使用。

地圖適配器實例

步驟

1. 在驗證來源對應標籤上，選擇*對應新適配器實例*。
2. 在適配器實例標籤上，選擇適配器實例你創造的。
3. 在「映射方法」標籤上，選擇「從資料儲存體中檢索附加屬性」。
4. 在「屬性來源和使用者尋找」標籤上，選擇「新增屬性來源」。
5. 在資料儲存標籤上，提供描述並選擇資料儲存你補充道。
6. 在 LDAP 目錄搜尋標籤上：
   - 輸入*Base DN*，它應該與您在StorageGRID中為 LDAP 伺服器輸入的值完全相符。
   - 對於搜尋範圍，選擇*子樹*。
   - 對於根物件類，搜尋並新增以下任一屬性：**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 過濾器標籤上，輸入 **sAMAccountName=${username}**。
9. 在“屬性合約履行”標籤上，從“來源”下拉選單中選擇“**LDAP**（屬性）”，然後從“值”下拉選單中選擇“**objectGUID**”或“**userPrincipalName**”。
10. 審查並保存屬性來源。
11. 在「Failsave Attribute Source」標籤上，選擇「**Abort the SSO Transaction**」。
12. 查看摘要並選擇*完成*。
13. 選擇*完成*。

配置協議設定

步驟

1. 在 * SP連線 * > * 瀏覽器 SSO * > * 協定設定 * 標籤上，選擇 * 設定協定設定 *。
2. 在斷言消費者服務 URL 標籤上，接受從StorageGRID SAML 元資料匯入的預設值（用於綁定和 `/api/saml-response`（用於端點 URL）。
3. 在 SLO 服務 URL 標籤上，接受從StorageGRID SAML 元資料匯入的預設值（用於綁定和 `/api/saml-logout` 用於端點 URL。
4. 在允許的 SAML 綁定標籤上，清除 **ARTIFACT** 和 **SOAP**。只需要 **POST** 和 **REDIRECT**。
5. 在「簽章原則」標籤上，勾選「要求對身分驗證要求進行簽署」和「始終簽署斷言」複選框。
6. 在加密策略標籤上，選擇*無*。
7. 查看摘要並選擇*完成*以儲存協定設定。
8. 查看摘要並選擇*完成*以儲存瀏覽器 SSO 設定。

配置憑證

步驟

1. 從SP連線標籤中，選擇 憑證。
2. 從「憑證」標籤中，選擇「配置憑證」。
3. 選擇簽署證書您建立或匯入的。
4. 選擇*下一步*進入*管理簽名驗證設定*。
   a. 在「信任模型」標籤上，選擇「**Unanchored**」。
   b. 在「簽署驗證憑證」標籤上，檢視從StorageGRID SAML 元資料匯入的簽名憑證資訊。
5. 查看摘要畫面並選擇*儲存*以儲存SP連線。

建立其他**SP**連接

您可以複製第一個SP連線來為網格中的每個管理節點建立所需的SP連線。您為每個副本上傳新的元資料。

> 不同管理節點的SP連線使用相同的設置，但合作夥伴的實體 ID、基本 URL、連線 ID、連線名稱、簽章驗證和 SLO 回應 URL 除外。

步驟

1. 選擇「操作」>「複製」為每個附加管理節點建立初始SP連線的副本。
2. 輸入副本的連線 ID 和連線名稱，然後選擇*儲存*。
3. 選擇與管理節點對應的元資料檔：
   a. 選擇*操作* > 使用元資料更新。
   b. 選擇*選擇檔案*並上傳元資料。
   c. 選擇“下一步”。
   d. 選擇*儲存*。
4. 解決由於未使用屬性而導致的錯誤：
   a. 選擇新的連接。
   b. 選擇*設定瀏覽器 SSO > 設定斷言建立 > 屬性契約*。
   c. 刪除 **urn:oid** 的條目。
   d. 選擇*儲存*。

停用單一登入

如果您不再想使用此功能，可以停用單一登入 (SSO)。您必須先停用單一登錄，然後才能停用身份聯合。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

步驟

1. 選擇*設定* > 存取控制 > 單一登入。

出現「單一登入」頁面。

2. 選擇“已停用”選項。
3. 選擇*儲存*。

   出現警告訊息，表示本地用戶現在可以登入。

4. 選擇“確定”。

   下次登入StorageGRID時，將出現StorageGRIDSign in頁面，您必須輸入本機或聯合StorageGRID使用者的使用者名稱和密碼。

暫時停用並重新啟用一個管理節點的單一登入

如果單一登入 (SSO) 系統發生故障，您可能無法登入網格管理員。在這種情況下，您可以暫時停用並重新啟用一個管理節點的 SSO。若要停用然後重新啟用 SSO，您必須存取節點的命令 shell。

開始之前

- 你有"特定存取權限"。
- 你有 `Passwords.txt`文件。
- 您知道本機 root 使用者的密碼。

關於此任務

停用一個管理節點的 SSO 後，您可以以本機 root 使用者身分登入網格管理員。為了保護您的StorageGRID系統，您必須在登出後立即使用節點的命令 shell 在管理節點上重新啟用 SSO。

> 停用一個管理節點的 SSO 不會影響網格中任何其他管理節點的 SSO 設定。網格管理器中單一登入頁面上的「啟用 SSO」複選框保持選取狀態，並且所有現有的 SSO 設定都將保留，除非您更新它們。

步驟

1. 登入管理節點：
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

      當您以 root 身分登入時，提示字元將從 `$`到 `#`。

2. 運行以下命令：`disable-saml`

   一條訊息表明該命令僅適用於此管理節點。

3. 確認您要停用 SSO。

一則訊息表示該節點上的單一登入已停用。

4. 從 Web 瀏覽器存取相同管理節點上的網格管理器。

   由於 SSO 已停用，因此現在顯示 Grid Manager 登入頁面。

5. 使用使用者名稱 root 和本機 root 使用者的密碼Sign in。
6. 如果您因為需要更正 SSO 設定而暫時停用了 SSO：
   a. 選擇*設定* > 存取控制 > 單一登入。
   b. 更改不正確或過時的 SSO 設定。
   c. 選擇*儲存*。

      從單一登入頁面選擇「儲存」會自動為整個網格重新啟用 SSO。

7. 如果您因其他原因需要存取網格管理員而暫時停用了 SSO：
   a. 執行您需要執行的任何任務。
   b. 選擇*退出*，然後關閉網格管理員。
   c. 在管理節點上重新啟用 SSO。您可以執行下列任何步驟：

      - 運行以下命令： `enable-saml`

        一條訊息表明該命令僅適用於此管理節點。

      確認您要啟用 SSO。

   一則訊息表示該節點上已啟用單一登入。

   - 重新啟動網格節點： `reboot`

8. 透過 Web 瀏覽器，從同一個管理節點存取網格管理器。
9. 確認出現StorageGRIDSign in頁面，並且您必須輸入 SSO 憑證才能存取網格管理員。