控制StorageGRID 對功能的存取

StorageGRID 11.8

NetApp
May 10, 2024

目錄

控制StorageGRID 對功能的存取

控制 StorageGRID 存取：總覽

您可以透過StorageGRID 建立或匯入群組和使用者、並指派權限給每個群組、來控制哪些人可以存取功能、以及使用者可以執行哪些工作。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

您可以透過從身分識別聯盟服務匯入群組和使用者、或設定本機群組和本機使用者、來判斷誰可以存取Grid Manager和Grid Management API。

使用 "身分識別聯盟" 進行設定 "群組" 和 "使用者" 更快、而且使用者可以使用熟悉的認證登入 StorageGRID 。如果您使用Active Directory、OpenLDAP或Oracle Directory Server、則可以設定身分識別聯盟。

如果您想要使用另一項LDAP v3服務、請聯絡技術支援部門。

您可以指派不同的工作來決定每個使用者可以執行哪些工作 "權限" 給每個群組。例如、您可能希望某個群組中的使用者能夠管理ILM規則、以及其他群組中的使用者執行維護工作。使用者必須屬於至少一個群組才能存取系統。

您也可以將群組設定為唯讀。唯讀群組中的使用者只能檢視設定和功能。他們無法在 Grid Manager 或 Grid Management API 中進行任何變更或執行任何作業。

啟用單一登入

支援使用安全聲明標記語言2.0（SAML 2.0）標準的單一登入（SSO）StorageGRID 。您先請 "設定並啟用SSO"、所有使用者必須先由外部身分識別供應商驗證、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 。

變更資源配置複雜密碼

許多安裝與維護程序、以及下載StorageGRID 「還原套件」時、都需要使用資源配置密碼。也需要通關密碼才能下載適用於StorageGRID 整個系統的網格拓撲資訊和加密金鑰備份。您可以 "變更複雜密碼" 視需要而定。

變更節點主控台密碼

網格中的每個節點都有唯一的節點主控台密碼、您必須以「 admin 」的身分使用 SSH 登入節點、或是以 VM/實體主控台連線的根使用者登入。如有需要、您可以 "變更節點主控台密碼" 針對每個節點。

變更資源配置通關密碼

請使用此程序來變更StorageGRID 供應密碼。恢復、擴充和維護程序需要通關密碼。下載「恢復套件」備份時、也需要密碼、其中包括網格拓撲資訊、網格節點主控台密碼、StorageGRID 以及適用於該系統的加密金鑰。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您具有「維護」或「根」存取權限。
- 您有目前的資源配置通關密碼。

關於這項工作

許多安裝和維護程序以及的都需要資源配置通關密碼 "正在下載恢復套件"。中未列出資源配置通關密碼 `Passwords.txt` 檔案：請務必記錄資源配置通關密碼、並將密碼保存在安全的位置。

步驟

1. 選擇*組態*>*存取控制*網格密碼。
2. 在 * 變更資源配置密碼 * 下、選取 * 進行變更 *
3. 輸入您目前的資源配置通關密碼。
4. 輸入新的通關密碼。通關密碼必須包含至少8個字元、且不得超過32個字元。密碼區分大小寫。
5. 將新的資源配置通關密碼儲存在安全的位置。安裝、擴充和維護程序都必須如此。
6. 重新輸入新的通關密碼、然後選取*「Save*（儲存*）」。

   資源配置通關密碼變更完成時、系統會顯示綠色的成功標語。

7. 選擇*恢復套件*。
8. 輸入新的資源配置密碼以下載新的恢復套件。

   變更資源配置通關密碼之後、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。

變更節點主控台密碼

網格中的每個節點都有唯一的節點主控台密碼、您必須登入節點。請使用這些步驟來變更網格中每個節點的每個唯一節點主控台密碼。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "維護或根存取權限"。
- 您有目前的資源配置通關密碼。

關於這項工作

使用節點主控台密碼、以「 admin 」身分使用 SSH 登入節點、或以 VM/ 實體主控台連線的 root 使用者身分登入。變更節點主控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中 `Passwords.txt` 恢復套件中的檔案。密碼會列在Passwords.txt檔案的「Password（密碼）」欄中。

SSH金鑰有個別的SSH存取密碼、用於節點之間的通訊。此程序不會變更 SSH 存取密碼。

存取精靈

步驟

1. 選擇*組態*>*存取控制*>*網格密碼*。
2. 在 * 變更節點主控台密碼 * 下、選取 * 進行變更 * 。

輸入資源配置通關密碼

步驟

1. 輸入您網格的資源配置密碼。
2. 選擇*繼續*。

下載目前的恢復套件

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. 選擇*下載恢復套件*。
2. 複製恢復套件檔案 (`.zip`）到兩個安全、安全且獨立的位置。

   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。

3. 選擇*繼續*。
4. 當確認對話方塊出現時、如果您已準備好開始變更節點主控台密碼、請選取 * 是 * 。

   您無法在程序啟動後取消此程序。

變更節點主控台密碼

當節點主控台密碼程序啟動時、會產生新的還原套件、其中包含新密碼。然後、每個節點上的密碼都會更新。

步驟

1. 等待產生新的恢復套件、這可能需要幾分鐘的時間。
2. 選擇*下載新的恢復套件*。
3. 下載完成時：
   a. 開啟 `.zip` 檔案：
   b. 確認您可以存取內容、包括 `Passwords.txt` 檔案、其中包含新節點主控台密碼。
   c. 複製新的恢復套件檔案 (`.zip`）到兩個安全、安全且獨立的位置。

請勿覆寫舊的恢復套件。

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. 選取核取方塊、表示您已下載新的恢復套件並驗證內容。
5. 選取 * 變更節點主控台密碼 * 、並等待所有節點以新密碼更新。這可能需要幾分鐘的時間。

   如果變更所有節點的密碼、會出現綠色的成功橫幅。前往下一步。

   如果在更新程序期間發生錯誤、則會出現橫幅訊息、列出無法變更密碼的節點數量。系統會在任何無法變更密碼的節點上、自動重試此程序。如果程序結束時、部分節點仍未變更密碼、則會出現*重試*按鈕。

   如果一或多個節點的密碼更新失敗：

   a. 檢閱表中所列的錯誤訊息。
   b. 解決問題。
   c. 選擇*重試*。

      重試只會變更先前密碼變更嘗試期間失敗之節點上的節點主控台密碼。

6. 變更所有節點的節點主控台密碼後、請刪除 您下載的第一個恢復套件。
7. 您也可以選擇使用 * 恢復套件 * 連結來下載新恢復套件的其他複本。

使用身分識別聯盟

使用身分識別聯盟可更快設定群組和使用者、並讓使用者StorageGRID 使用熟悉的認證登入到這個功能。

設定Grid Manager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）中管理系統管理群組和使用者、可以在Grid Manager中設定身分識別聯盟。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 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。
- 如果您打算啟用單一登入（SSO）、則已檢閱 "單一登入的要求與考量"。
- 如果您打算使用傳輸層安全性（TLS）與LDAP伺服器進行通訊、則身分識別供應商使用的是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

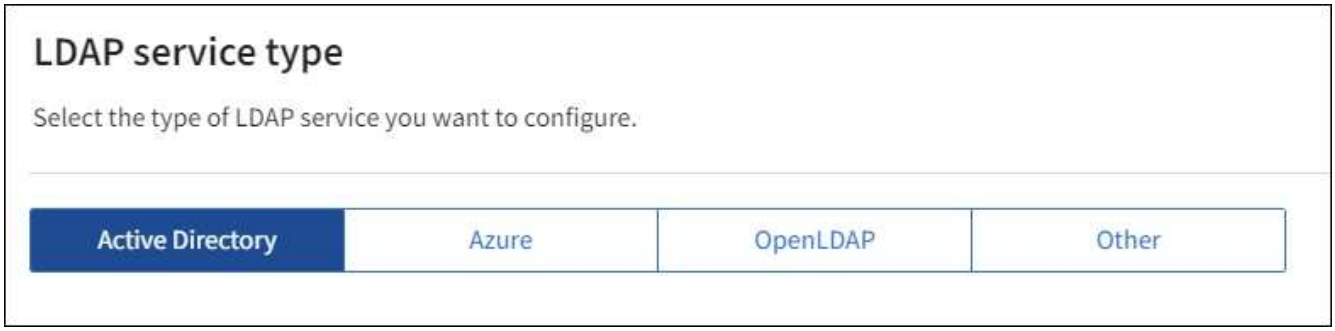
如果您想從其他系統（例如Active Directory、Azure AD、OpenLDAP或Oracle Directory Server）匯入群組、可以設定Grid Manager的身分識別來源。您可以匯入下列群組類型：

- 管理群組：管理群組中的使用者可以登入Grid Manager、並根據指派給群組的管理權限來執行工作。
- 不使用其本身身分識別來源的租戶使用者群組。租戶群組中的使用者可以登入租戶管理程式、並根據在租戶管理程式中指派給群組的權限來執行工作。請參閱 "建立租戶帳戶" 和 "使用租戶帳戶" 以取得詳細資料。

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 `sAMAccountName` 適用於Active Directory和 `uid` 適用於OpenLDAP。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 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定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、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 `sAMAccountName` 適用於Active Directory和 `cn` 適用於OpenLDAP。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 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `nsuniqueid`。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：

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

- 密碼：與使用者名稱相關的密碼。

  如果您在未來變更密碼、您必須在此頁面上更新密碼。

- 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）：如果無法自動判斷模式、則應使用預設的使用者名稱模式StorageGRID 。

  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：

  - * UserPrincipalName 模式（ Active Directory 和 Azure ） * ： `[USERNAME]@example.com`
  - * 低階登入名稱模式（ Active Directory 和 Azure ） * ： `example\[USERNAME]`
  - * 辨別名稱模式 * ： `CN=[USERNAME],CN=Users,DC=example,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。

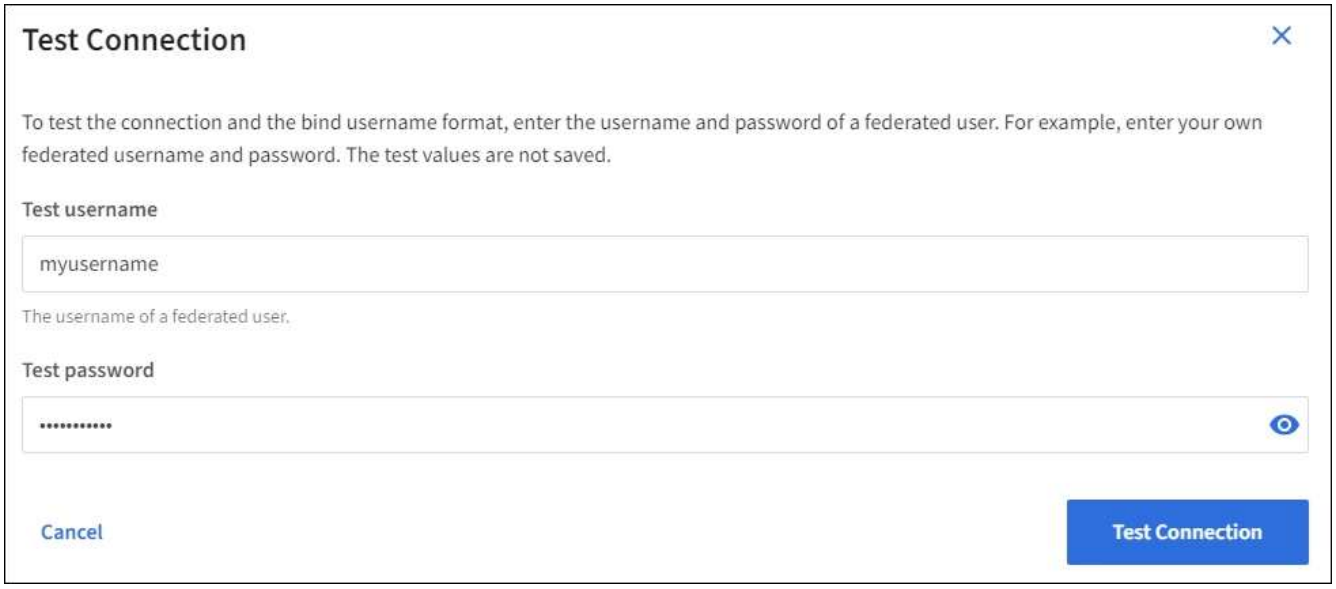
測試連線並儲存組態

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

步驟

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、就會出現「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、就會出現「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、就會出現「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。
- 如果將單點登錄 (SSO) 設置爲 **Enabled** 或 **Sandbox Mode** ，則禁用 **Enable identity Federation** （啓用身份聯合） * 複選框。「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. 取消勾選 * 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 不會自動封鎖 S3 對外部停用使用者的存取。若要封鎖 S3 存取、請刪除使用者的任何 S3 金鑰、或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 "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 "OpenLDAP文件：2.4版管理員指南"。

管理管理群組

您可以建立管理群組、以管理一或多個管理使用者的安全性權限。使用者必須屬於某個群組、才能獲得StorageGRID 存取該系統的權限。

開始之前

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

建立管理群組

管理群組可讓您決定哪些使用者可以存取Grid Manager和Grid Management API中的哪些功能和作業。

存取精靈

步驟

1. 選擇*組態*>*存取控制*>*管理群組*。
2. 選取*建立群組*。

選擇群組類型

您可以建立本機群組或匯入同盟群組。

- 如果您要指派權限給本機使用者、請建立本機群組。
- 建立聯盟群組、從身分識別來源匯入使用者。

本機群組

步驟

1. 選擇*本機群組*。
2. 輸入群組的顯示名稱、您可視需要稍後更新。例如「維護使用者」或「 ILM 管理員」。
3. 輸入群組的唯一名稱、您稍後無法更新。
4. 選擇*繼續*。

聯盟群組

步驟

1. 選取*聯盟群組*。
2. 輸入您要匯入的群組名稱、完全如同在設定的身分識別來源中所顯示的名稱。
   - 對於Active Directory和Azure、請使用sAMAccountName。
   - 若為OpenLDAP、請使用「CN"（通用名稱）」。
   - 對於另一個LDAP、請為LDAP伺服器使用適當的唯一名稱。
3. 選擇*繼續*。

管理群組權限

步驟

1. 若為*存取模式*、請選取群組中的使用者是否可以在Grid Manager和Grid Management API中變更設定及執行作業、或是只能檢視設定和功能。
   - 讀寫（預設）：使用者可以變更設定、並執行其管理權限所允許的作業。
   - 唯讀：使用者只能檢視設定和功能。他們無法在 Grid Manager 或 Grid Management 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。

     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。

2. 選取一或多個 "管理群組權限"。

   您必須為每個群組指派至少一項權限、否則屬於該群組的使用者將無法登入StorageGRID 。

3. 如果您要建立本機群組、請選取*繼續*。如果您要建立聯盟群組、請選取*建立群組*和*完成*。

新增使用者（僅限本機群組）

步驟

1. 您也可以為此群組選取一或多個本機使用者。

   如果您尚未建立本機使用者、可以儲存群組而不新增使用者。您可以將此群組新增至「使用者」頁面上的使用者。請參閱 "管理使用者" 以取得詳細資料。

2. 選擇* Create group（創建組）和 Finish（完成）*。

檢視及編輯管理群組

您可以檢視現有群組的詳細資料、修改群組或複製群組。

- 若要檢視所有群組的基本資訊、請檢閱「群組」頁面上的表格。
- 若要檢視特定群組的所有詳細資料或編輯群組、請使用*「動作」*功能表或「詳細資料」頁面。

工作	「行動」功能表	詳細資料頁面
檢視群組詳細資料	a. 選取群組的核取方塊。 b. 選取*「動作*」>*「檢視群組詳細資料*」。	在表格中選取群組名稱。
編輯顯示名稱（僅限本機群組）	a. 選取群組的核取方塊。 b. 選擇*操作*>*編輯群組名稱*。 c. 輸入新名稱。 d. 選取*儲存變更*。	a. 選取群組名稱以顯示詳細資料。 b. 選取編輯圖示 。 c. 輸入新名稱。 d. 選取*儲存變更*。
編輯存取模式或權限	a. 選取群組的核取方塊。 b. 選取*「動作*」>*「檢視群組詳細資料*」。 c. 或者、變更群組的存取模式。 d. 或者、選取或清除 "管理群組權限"。 e. 選取*儲存變更*。	a. 選取群組名稱以顯示詳細資料。 b. 或者、變更群組的存取模式。 c. 或者、選取或清除 "管理群組權限"。 d. 選取*儲存變更*。

複製群組

步驟

1. 選取群組的核取方塊。
2. 選取*「動作*」>*「重複群組*」。
3. 完成「複製群組」精靈。

刪除群組

當您想要從系統中移除群組時、可以刪除管理群組、並移除與群組相關的所有權限。刪除管理群組會移除群組中的任何使用者、但不會刪除使用者。

步驟

1. 在「群組」頁面中、選取您要移除的每個群組的核取方塊。
2. 選擇*操作*>*刪除群組*。
3. 選擇*刪除群組*。

管理群組權限

建立管理使用者群組時、您可以選取一或多個權限來控制對Grid Manager特定功能的存取。然後、您可以將每個使用者指派給一或多個這些管理群組、以決定使用者可以執行哪些工作。

您必須為每個群組指派至少一項權限、否則屬於該群組的使用者將無法登入Grid Manager或Grid Management API。

根據預設、任何屬於至少擁有一項權限之群組的使用者、都可以執行下列工作：

- 登入Grid Manager
- 檢視儀表板
- 檢視節點頁面
- 監控網格拓撲
- 檢視目前和已解決的警示
- 檢視目前和歷史警報（舊系統）
- 變更自己的密碼（僅限本機使用者）
- 檢視「組態與維護」頁面上提供的特定資訊

權限與存取模式之間的互動

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、或是只能檢視相關的設定與功能。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。

下列各節將說明您在建立或編輯管理群組時可以指派的權限。任何未明確提及的功能都需要*根存取*權限。

root存取權

此權限可讓您存取所有網格管理功能。

認可警示（舊版）

此權限可讓您存取「Acknowledge and回應警示（舊系統）」。所有登入的使用者都可以檢視目前和歷史警報。

如果您希望使用者僅監控網格拓撲並認可警示、則應指派此權限。

變更租戶根密碼

此權限可讓您存取「租戶」頁面上的*變更root密碼*選項、讓您控制誰可以變更租戶本機root使用者的密碼。啟用S3金鑰匯入功能時、此權限也可用於移轉S3金鑰。沒有此權限的使用者無法看到 * 變更 root 密碼 * 選項。

若要授予「租戶」頁面的存取權（包含*變更root密碼*選項）、請同時指派*租戶帳戶*權限。

網格拓撲頁面組態

此權限可讓您存取「支援>*工具*>*網格拓撲*」頁面上的「組態」索引標籤。

ILM

此權限可讓您存取下列* ILM *功能表選項：

- 規則
- 原則
- 銷毀編碼
- 區域
- 儲存資源池

使用者必須擁有*其他網格組態*和*網格拓撲頁面組態*權限、才能管理儲存等級。

維護

使用者必須擁有維護權限、才能使用下列選項：

- 組態>*存取控制*：
  - 網格密碼
- 組態>*網路*：
  - S3 端點網域名稱
- 維護>*工作*：
  - 取消委任
  - 擴充
  - 物件存在檢查
  - 恢復
- 維護>*系統*：
  - 恢復套件
  - 軟體更新
- 支援>*工具*：
  - 記錄

沒有維護權限的使用者可以檢視但無法編輯這些頁面：

- 維護>*網路*：
  - DNS伺服器
  - 網格網路

- NTP 伺服器

- 維護>*系統*：
  - 授權
- 組態>*網路*：
  - S3 端點網域名稱
- 組態>*安全性*：
  - 憑證
- 組態>*監控*：
  - 稽核與syslog伺服器

管理警示

此權限可讓您存取管理警示的選項。使用者必須擁有此權限、才能管理靜音、警示通知及警示規則。

度量查詢

此權限可讓您存取：

- * 支援 * > * 工具 * > * 指標 * 頁面
- 使用 Grid Management API 的 * Metrics * 區段來自訂 Prometheus 指標查詢
- 包含計量的 Grid Manager 儀表板卡

物件中繼資料查詢

此權限可讓您存取「* ILM >*物件中繼資料查詢」頁面。

其他網格組態

此權限可讓您存取其他網格組態選項。

若要查看這些額外選項、使用者也必須具有* Grid拓撲頁面組態*權限。

- * ILM *：
  - 儲存等級
- 組態>*系統*：
  - 儲存選項
- 支援>*警示（舊版）*：
  - 自訂事件
  - 全域警示
  - 舊版電子郵件設定
- * 支援 * > * 其他 * ：

- 連結成本

儲存應用裝置管理員

此權限提供：

- 透過 Grid Manager 存取儲存設備上的 E 系列 SANtricity 系統管理員。
- 可在支援這些作業的應用裝置的「管理磁碟機」索引標籤上執行疑難排解和維護工作。

租戶帳戶

此權限可讓您：

- 存取租戶頁面、您可以在其中建立、編輯及移除租戶帳戶
- 檢視現有的流量分類原則
- 檢視包含租戶詳細資料的 Grid Manager 儀表板卡

管理使用者

您可以檢視本機和聯盟使用者。您也可以建立本機使用者、並將其指派給本機管理群組、以決定這些使用者可以存取哪些Grid Manager功能。

開始之前

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

建立本機使用者

您可以建立一或多個本機使用者、並將每個使用者指派給一或多個本機群組。群組的權限可控制使用者可以存取的Grid Manager和Grid Management API功能。

您只能建立本機使用者。使用外部身分識別來源來管理同盟使用者和群組。

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。

如果啟用單一登入（ SSO ）、本機使用者將無法登入 StorageGRID 。

存取精靈

步驟

1. 選擇*組態*>*存取控制*>*管理使用者*。
2. 選取*建立使用者*。

輸入使用者認證資料

步驟

1. 輸入使用者的全名、唯一使用者名稱及密碼。
2. 或者、如果此使用者不應存取Grid Manager或Grid Management API、請選取* Yes*。
3. 選擇*繼續*。

指派給群組

步驟

1. 或者、將使用者指派給一或多個群組、以決定使用者的權限。

   如果您尚未建立群組、可以儲存使用者而不選取群組。您可以將此使用者新增至「群組」頁面上的群組。

   如果使用者屬於多個群組、則權限會累計。請參閱 "管理管理群組" 以取得詳細資料。

2. 選擇* Create user*（創建用戶*）並選擇* Finish（完成）*。

檢視及編輯本機使用者

您可以檢視現有本機和聯盟使用者的詳細資料。您可以修改本機使用者、以變更使用者的完整名稱、密碼或群組成員資格。您也可以暫時禁止使用者存取Grid Manager和Grid Management API。

您只能編輯本機使用者。使用外部身分識別來源來管理同盟使用者。

- 若要檢視所有本機和聯盟使用者的基本資訊、請檢閱「使用者」頁面上的表格。
- 若要檢視特定使用者的所有詳細資料、編輯本機使用者、或變更本機使用者的密碼、請使用* Actions（動作）*功能表或詳細資料頁面。

  使用者下次登出並重新登入Grid Manager時、即會套用任何編輯內容。

  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。

工作	「行動」功能表	詳細資料頁面
檢視使用者詳細資料	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料	在表格中選取使用者名稱。
編輯全名（僅限本機使用者）	a. 選取使用者的核取方塊。 b. 選擇* Actions > Edit full name*（操作>*編輯全名*）。 c. 輸入新名稱。 d. 選取*儲存變更*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取編輯圖示 。 c. 輸入新名稱。 d. 選取*儲存變更*。

工作	「行動」功能表	詳細資料頁面
拒絕StorageGRID或允許存取	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料 c. 選取「存取」索引標籤。 d. 選取*是*以防止使用者登入Grid Manager或Grid Management API、或選取*否*以允許使用者登入。 e. 選取*儲存變更*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取「存取」索引標籤。 c. 選取*是*以防止使用者登入Grid Manager或Grid Management API、或選取*否*以允許使用者登入。 d. 選取*儲存變更*。
變更密碼（僅限本機使用者）	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料 c. 選取密碼索引標籤。 d. 輸入新密碼。 e. 選擇*變更密碼*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取密碼索引標籤。 c. 輸入新密碼。 d. 選擇*變更密碼*。
變更群組（僅限本機使用者）	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料 c. 選取群組索引標籤。 d. 或者、選取群組名稱後的連結、即可在新的瀏覽器索引標籤中檢視群組的詳細資料。 e. 選取*編輯群組*以選取不同的群組。 f. 選取*儲存變更*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取群組索引標籤。 c. 或者、選取群組名稱後的連結、即可在新的瀏覽器索引標籤中檢視群組的詳細資料。 d. 選取*編輯群組*以選取不同的群組。 e. 選取*儲存變更*。

複製使用者

您可以複製現有使用者、以建立具有相同權限的新使用者。

步驟

1. 選取使用者的核取方塊。
2. 選取*「動作*」>*「重複使用者*」。
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、將該使用者從系統中永久移除。

您無法刪除 root 使用者。

步驟

1. 在「使用者」頁面中、選取您要移除的每位使用者的核取方塊。
2. 選取*「動作*」>*「刪除使用者*」。
3. 選擇*刪除使用者*。

使用單一登入（SSO）

設定單一登入

啟用單一登入（SSO）時、如果使用者的認證是使用組織實作的SSO登入程序來授權、則只能存取Grid Manager、租戶管理程式、Grid Management API或租戶管理API。本機使用者無法登入 StorageGRID 。

單一登入的運作方式

支援使用安全聲明標記語言2.0（SAML 2.0）標準的單一登入（SSO）StorageGRID 。

在啟用單一登入（SSO）之前、請先檢閱StorageGRID 啟用SSO時、哪些地方會影響到「資訊登入」和「登出」程序。

啟用**SSO**時登入

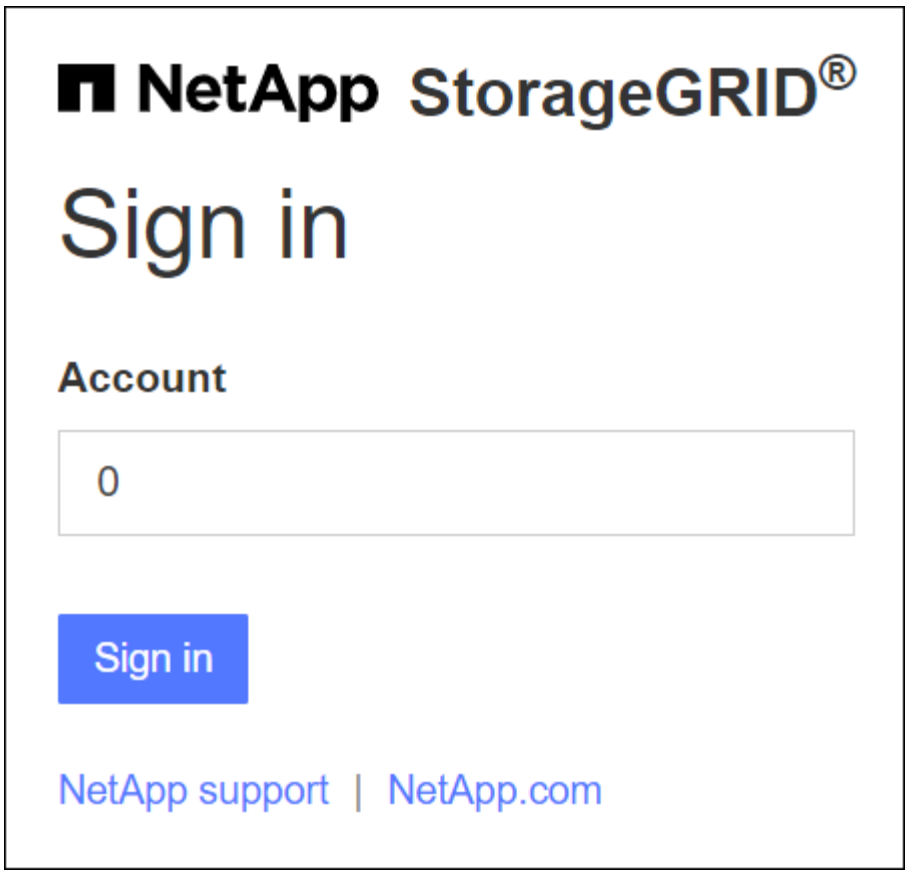
啟用SSO並登入StorageGRID 支援功能時、系統會將您重新導向至組織的SSO頁面、以驗證您的認證資料。

步驟

1. 在StorageGRID 網頁瀏覽器中輸入任何「靜態管理節點」的完整網域名稱或IP位址。

   畫面上會出現「簽署」頁面。StorageGRID

   - 如果這是您第一次存取此瀏覽器上的URL、系統會提示您輸入帳戶ID：

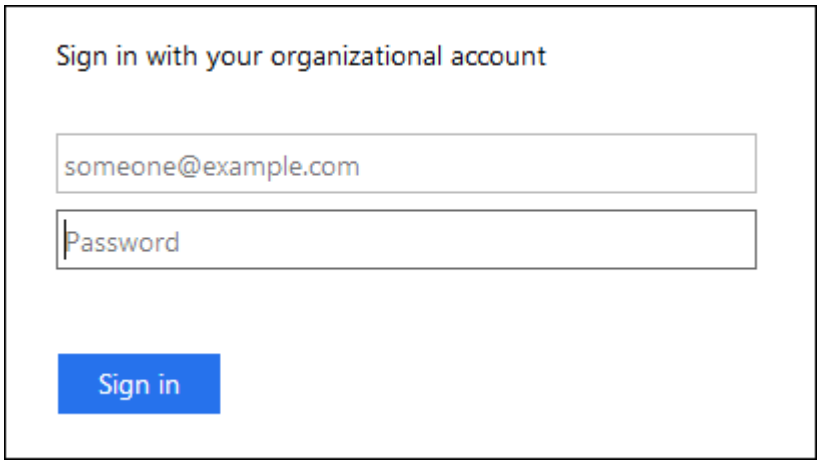


。如果您先前曾存取Grid Manager或Tenant Manager、系統會提示您選擇最近的帳戶或輸入帳戶ID：

輸入租戶帳戶的完整URL（即完整網域名稱或IP位址之後）時、不會顯示「協助登入」頁面StorageGRID `/?accountId=20-digit-account-id`）。而是會立即重新導向至組織的SSO登入頁面、您可以在其中登入 使用SSO認證登入。

2. 指出您要存取Grid Manager或租戶管理程式：
   - 若要存取Grid Manager、請將*帳戶ID*欄位保留空白、輸入* 0*作為帳戶ID、或選取* Grid Manager*（若出現在最近的帳戶清單中）。
   - 若要存取租戶管理程式、請輸入20位數的租戶帳戶ID、或是在最近的帳戶清單中、依名稱選取租戶。
3. 選擇*登入*

   可將您重新導向至組織的SSO登入頁面。StorageGRID例如：



4. [[signin_SSO]使用您的SSO認證登入。

   如果SSO認證資料正確：

   a. 身分識別供應商（IDP）提供驗證回應StorageGRID 功能以回應功能。
   b. 驗證驗證回應。StorageGRID
   c. 如果回應有效、且您屬於具有StorageGRID 下列存取權限的聯盟群組、您將會登入Grid Manager或租戶管理程式、視您選取的帳戶而定。

   > 如果無法存取服務帳戶、您仍可登入、只要您是擁有StorageGRID 存取權限之聯盟群組的現有使用者。

5. 您也可以存取其他管理節點、或是存取Grid Manager或租戶管理程式（如果您有足夠的權限）。

   您不需要重新輸入 SSO 認證。

啟用SSO時登出

啟用SSO以StorageGRID 利執行功能時、登出時會發生什麼事取決於您登入的項目、以及登出的位置。

步驟

1. 在使用者介面右上角找到 * 登出 * 連結。
2. 選取 * 登出 * 。

   畫面上會出現「簽署」頁面。StorageGRID「最近的帳戶」下拉式清單會更新為包含* Grid Manager*或租戶名稱、以便日後更快存取這些使用者介面。

如果您已登入...	您也可以登出...	您已登出...
一個或多個管理節點上的Grid Manager	任何管理節點上的Grid Manager	所有管理節點上的Grid Manager *附註：*如果您使用Azure進行SSO、可能需要幾分鐘的時間才能登出所有管理節點。
一或多個管理節點上的租戶管理程式	任何管理節點上的租戶管理程式	所有管理節點上的租戶管理程式
Grid Manager與租戶管理程式	網格管理程式	僅限Grid Manager。您也必須登出租戶管理程式、才能登出SSO。

下表摘要說明當您使用單一瀏覽器工作階段登出時會發生的情況。如果您在StorageGRID 多個瀏覽器工作階段之間登入到Sof、則必須分別登出所有瀏覽器工作階段。

單一登入的要求與考量

為 StorageGRID 系統啟用單一登入（ SSO ）之前、請先檢閱需求和考量事項。

身分識別供應商要求

支援下列SSO身分識別供應商（IDP）StorageGRID ：

- Active Directory Federation Service（AD FS）
- Azure Active Directory（Azure AD）
- PingFedate

您必須先為StorageGRID 您的支援系統設定身分識別聯盟、才能設定SSO身分識別供應商。您用於身分識別聯盟的LDAP服務類型會控制您可以實作的SSO類型。

已設定的**LDAP**服務類型	**SSO**身分識別供應商選項
Active Directory	• Active Directory • Azure • PingFedate
Azure	Azure

AD FS需求

您可以使用下列任何版本的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"或更高版本。

其他需求

- 傳輸層安全性（TLS）1.2或1.3
- Microsoft .NET Framework版本3.5.1或更新版本

Azure 的考量

如果您使用 Azure 做為 SSO 類型、且使用者的使用者主體名稱不使用 sAMAccountName 做為首碼、則當 StorageGRID 失去與 LDAP 伺服器的連線時、可能會發生登入問題。若要允許使用者登入、您必須還原與 LDAP 伺服器的連線。

伺服器憑證需求

根據預設、StorageGRID 在每個管理節點上使用管理介面憑證、以安全存取Grid Manager、租戶管理程式、Grid Management API及租戶管理API。當您設定依賴方信任（AD FS）、企業應用程式（Azure）或服務供應商連線（PingFedate）以供StorageGRID 進行時、您可以使用伺服器憑證做為StorageGRID 簽署憑證來執行Sfor Suse要求。

如果您還沒有 "已為管理介面設定自訂憑證"您現在應該這麼做。當您安裝自訂伺服器憑證時、它會用於所有管理節點、您可以在StorageGRID 所有依賴方信任、企業應用程式或SP連線中使用。

> 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、而您要將其恢復、則會產生新的預設伺服器憑證。在登入還原的節點之前、您必須使用新的憑證來更新依賴方信任、企業應用程式或SP連線。

您可以登入節點的命令Shell並前往、以存取管理節點的伺服器憑證 `/var/local/mgmt-api` 目錄。自訂伺服器憑證即會命名 `custom-server.crt`。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）無法在受限網格管理器或租戶管理器連接埠上使用。如果您想要使用者透過單一登入進行驗證、則必須使用預設的HTTPS連接埠（443）。請參閱 "控制外部防火牆的存取"。

確認同盟使用者可以登入

啟用單一登入（SSO）之前、您必須確認至少有一位同盟使用者可以登入Grid Manager、並登入任何現有租戶帳戶的租戶管理程式。

開始之前

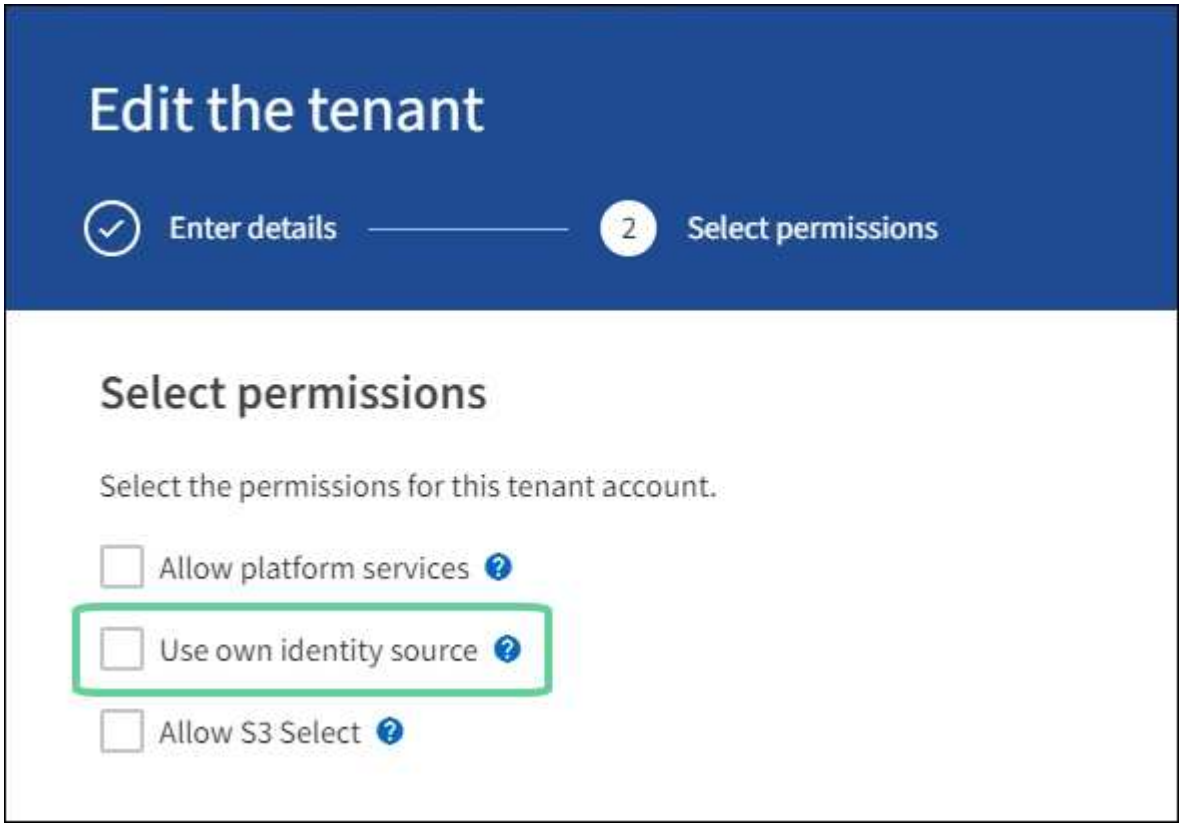
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已設定身分識別聯盟。

步驟

1. 如果有現有的租戶帳戶、請確認沒有租戶使用自己的身分識別來源。

> 啟用SSO時、在租戶管理程式中設定的身分識別來源會被在Grid Manager中設定的身分識別來源覆寫。屬於租戶身分識別來源的使用者將無法再登入、除非他們擁有Grid Manager身分識別來源的帳戶。

   a. 登入每個租戶帳戶的租戶管理程式。
   b. 選擇*存取管理*>*身分識別聯盟*。
   c. 確認未選取 * 啟用身分識別聯盟 * 核取方塊。
   d. 如果是、請確認不再需要此租戶帳戶使用的任何聯盟群組、清除核取方塊、然後選取 * 儲存 * 。
2. 確認聯盟使用者可以存取Grid Manager：
   a. 從Grid Manager中、選取*組態*>*存取控制*>*管理群組*。
   b. 請確定至少已從Active Directory身分識別來源匯入一個同盟群組、而且已將其指派為「根」存取權限。
   c. 登出。
   d. 確認您可以以聯盟群組中的使用者身分重新登入Grid Manager。
3. 如果有現有的租戶帳戶、請確認擁有root存取權限的聯盟使用者可以登入：
   a. 從Grid Manager中選取*租戶*。
   b. 選取租戶帳戶、然後選取*「Actions」（動作）>「Edit」（編輯）*。
   c. 在Enter details（輸入詳細資料）選項卡上、選取* Continue（繼續）*。
   d. 如果選中 * 使用自己的身份來源 * 複選框，則取消選中該複選框並選擇 * 保存 * 。



隨即顯示「租戶」頁面。

a. 選取租戶帳戶、選取*登入*、然後以本機root使用者身分登入租戶帳戶。
b. 在租戶管理程式中、選取*存取管理*>*群組*。
c. 請確定至少已指派Grid Manager中的一個聯盟群組給此租戶的根存取權限。
d. 登出。
e. 確認您可以以同盟群組中的使用者身分重新登入租戶。

相關資訊

- "單一登入的要求與考量"
- "管理管理群組"
- "使用租戶帳戶"

使用沙箱模式

您可以使用沙箱模式來設定及測試單一登入（SSO）、然後再為StorageGRID 所有的使用者啟用。啟用SSO之後、您可以在需要變更或重新測試組態時、隨時返回沙箱模式。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 您已為StorageGRID 您的整套系統設定身分識別聯盟。
- 若為身分識別聯盟* LDAP服務類型*、您會根據您打算使用的SSO身分識別供應商、選擇Active Directory或Azure。

已設定的**LDAP**服務類型	**SSO**身分識別供應商選項
Active Directory	• Active Directory • Azure • PingFedate
Azure	Azure

關於這項工作

啟用SSO且使用者嘗試登入管理節點時StorageGRID 、將驗證要求傳送給SSO身分識別供應商。接著、SSO身分識別供應商會將驗證回應傳回StorageGRID 至原地、指出驗證要求是否成功。對於成功的要求：

- Active Directory或PingFedate的回應包含使用者的通用唯一識別碼（UUID）。
- Azure的回應包括使用者主要名稱（UPN）。

若要讓StorageGRID 服務供應商（服務供應商）和SSO身分識別供應商能夠安全地溝通使用者驗證要求、您必須在StorageGRID 支援中心中設定某些設定。接下來、您必須使用SSO身分識別供應商的軟體、為每個管理節點建立信賴方信任（AD FS）、企業應用程式（Azure）或服務供應商（PingFedate）。最後、您必須返

回StorageGRID 到支援SSO的功能。

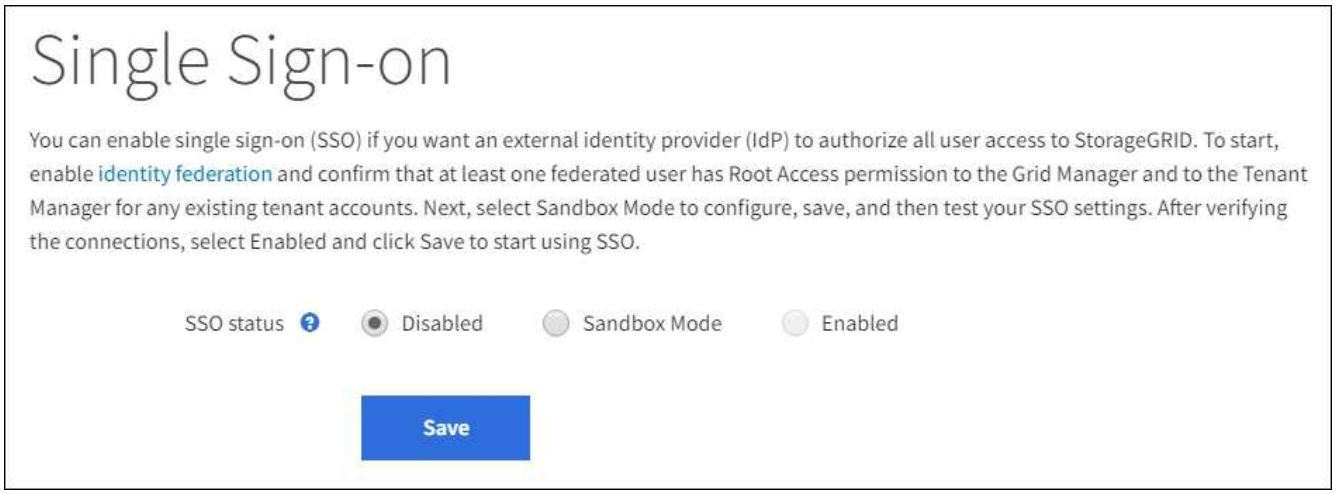
沙箱模式可讓您在啟用SSO之前、輕鬆執行此後端和後端組態、並測試所有設定。使用沙箱模式時、使用者無法使用 SSO 登入。

存取沙箱模式

步驟

1. 選擇*組態*>*存取控制*>*單一登入*。

   此時將顯示「單一登入」頁面、並選取「停用」選項。



   如果 SSO 狀態選項未出現、請確認您已將身分識別提供者設定為同盟身分識別來源。請參閱"單一登入的要求與考量"。

2. 選擇* Sandbox Mode*。

   此時會出現「身分識別提供者」區段。

輸入身分識別供應商詳細資料

步驟

1. 從下拉式清單中選取* SSO類型*。
2. 根據您選取的SSO類型、填寫「身分識別提供者」區段中的欄位。

Active Directory

1. 輸入身分識別提供者的*聯盟服務名稱*、完全如同Active Directory Federation Service（AD FS）中所示。

   若要尋找Federation服務名稱、請前往Windows Server Manager。選擇*工具*>* AD FS管理*。從「動作」功能表中選取*「編輯Federation Service內容」*。Federation Service名稱會顯示在第二個欄位中。

2. 指定當身分識別供應商傳送SSO組態資訊以回應StorageGRID 需求時、將使用哪些TLS憑證來保護連線安全。

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

     如果選取此設定、請複製自訂憑證的文字、然後貼到「* CA認證*」文字方塊中。

   - 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

     如果您變更 CA 憑證、請立即變更 "在管理節點上重新啟動 mgmt-API 服務" 並測試 Grid Manager 是否成功登入 SSO 。

3. 在「依賴方」區段中、指定* StorageGRID 依賴方識別符號*以供參考。此值可控制AD FS中每個依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、而且您預期未來不會新增更多管理節點、請輸入 `SG` 或 `StorageGRID`。
   - 如果網格包含多個管理節點、請加入字串 `[HOSTNAME]` 在識別碼中。例如、 `SG-[HOSTNAME]`。這會產生一個表格、根據節點的主機名稱、顯示系統中每個管理節點的依賴方識別碼。

   您必須為StorageGRID 您的系統中的每個管理節點建立信賴關係人信任關係。信任每個管理節點的依賴方、可確保使用者能夠安全地登入及登出任何管理節點。

4. 選擇*保存*。

   「儲存」按鈕上會出現綠色勾號幾秒鐘。

Azure

1. 指定當身分識別供應商傳送SSO組態資訊以回應StorageGRID 需求時、將使用哪些TLS憑證來保護連線安全。

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

     如果選取此設定、請複製自訂憑證的文字、然後貼到「* CA認證*」文字方塊中。

- 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

> 如果您變更 CA 憑證、請立即變更 "在管理節點上重新啟動 mgmt-API 服務" 並測試 Grid Manager 是否成功登入 SSO 。

2. 在「企業應用程式」區段中、指定*企業應用程式名稱* StorageGRID 以供參考。此值可控制Azure AD中每個企業應用程式所使用的名稱。

   - 例如、如果您的網格只有一個管理節點、而且您預期未來不會新增更多管理節點、請輸入 `SG` 或 `StorageGRID`。
   - 如果網格包含多個管理節點、請加入字串 `[HOSTNAME]` 在識別碼中。例如、 `SG-[HOSTNAME]`。這會產生一個表格、根據節點的主機名稱、顯示系統中每個管理節點的企業應用程式名稱。

> 您必須為StorageGRID 您的系統中的每個管理節點建立企業應用程式。為每個管理節點設定企業應用程式、可確保使用者安全地登入及登出任何管理節點。

3. 請依照中的步驟進行 "在Azure AD中建立企業應用程式" 為表格中所列的每個管理節點建立企業應用程式。
4. 從Azure AD複製每個企業應用程式的聯盟中繼資料URL。然後、將此URL貼到StorageGRID 相關的*聯盟中繼資料URL*欄位。
5. 複製並貼上所有管理節點的聯盟中繼資料URL之後、請選取*儲存*。

   「儲存」按鈕上會出現綠色勾號幾秒鐘。

PingFedate

1. 指定當身分識別供應商傳送SSO組態資訊以回應StorageGRID 需求時、將使用哪些TLS憑證來保護連線安全。

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

     如果選取此設定、請複製自訂憑證的文字、然後貼到「* CA認證*」文字方塊中。

   - 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

> 如果您變更 CA 憑證、請立即變更 "在管理節點上重新啟動 mgmt-API 服務" 並測試 Grid Manager 是否成功登入 SSO 。

2. 在「服務供應商（SP）」區段中、指定* SP連線ID* StorageGRID 以供參考。此值可控制您在PingFedate中用於每個SP連線的名稱。

   - 例如、如果您的網格只有一個管理節點、而且您預期未來不會新增更多管理節點、請輸入 `SG` 或 `StorageGRID`。
   - 如果網格包含多個管理節點、請加入字串 `[HOSTNAME]` 在識別碼中。例如、 `SG-[HOSTNAME]`。這會根據節點的主機名稱、產生一個表格、顯示系統中每個管理節點的SP連線ID。

您必須為StorageGRID 您的系統中的每個管理節點建立SP連線。為每個管理節點建立SP連線、可確保使用者安全地登入及登出任何管理節點。

3. 在*聯盟中繼資料URL*欄位中、指定每個管理節點的聯盟中繼資料URL。

   請使用下列格式：

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

4. 選擇*保存*。

   「儲存」按鈕上會出現綠色勾號幾秒鐘。

設定依賴方信任、企業應用程式或**SP**連線

儲存組態時、會出現沙箱模式確認通知。本通知確認沙箱模式已啟用、並提供概觀指示。

根據需要、可將其保留在沙箱模式中。StorageGRID不過、在「單一登入」頁面上選取*沙箱模式*時、所有StorageGRID 的支援項目都會停用SSO功能。只有本機使用者才能登入。

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

Active Directory

步驟

1. 移至Active Directory Federation Services（AD FS）。
2. 使用StorageGRID 「僅供單一登入」頁面上表所示的每個信賴方識別碼、建立一或多個可靠方的可靠信任。StorageGRID

   您必須為表格中顯示的每個管理節點建立一個信任關係。

   如需相關指示、請前往 "在AD FS中建立依賴方信任"。

Azure

步驟

1. 從您目前登入之管理節點的「單一登入」頁面、選取按鈕以下載並儲存SAML中繼資料。
2. 然後、針對網格中的任何其他管理節點、重複下列步驟：
   a. 登入節點。
   b. 選擇*組態*>*存取控制*>*單一登入*。
   c. 下載並儲存該節點的SAML中繼資料。
3. 前往Azure Portal。
4. 請依照中的步驟進行 "在Azure AD中建立企業應用程式" 將每個管理節點的SAML中繼資料檔案上傳至對應的Azure企業應用程式。

PingFedate

步驟

1. 從您目前登入之管理節點的「單一登入」頁面、選取按鈕以下載並儲存SAML中繼資料。
2. 然後、針對網格中的任何其他管理節點、重複下列步驟：
   a. 登入節點。
   b. 選擇*組態*>*存取控制*>*單一登入*。
   c. 下載並儲存該節點的SAML中繼資料。
3. 前往PingFedate。
4. "建立一個或多個StorageGRID 服務供應商（SP）連線以供使用"。使用每個管理節點的SP連線ID（如StorageGRID 「支援單一登入」頁面表格所示）、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**SSO**連線

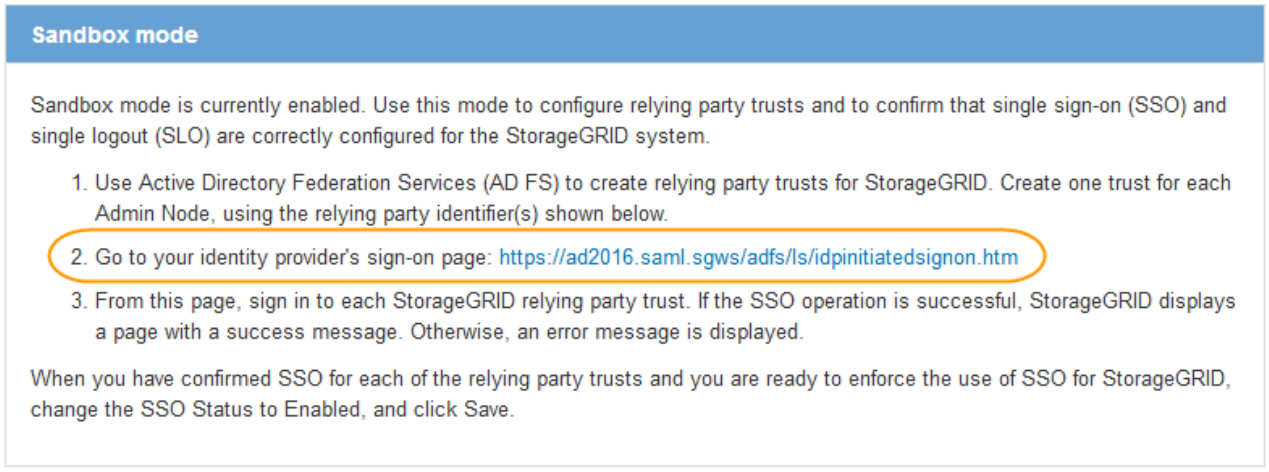
在您為整個StorageGRID 作業系統強制使用單一登入之前、您應確認已為每個管理節點正確設定單一登入和單一登出。

Active Directory

步驟

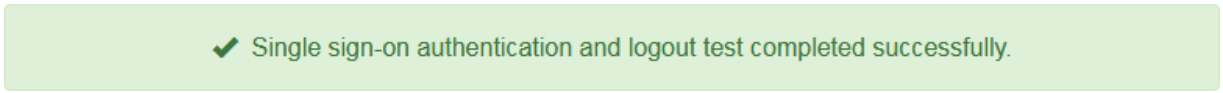
1. 從「功能表單一登入」頁面、找到沙箱模式訊息中的連結。StorageGRID

   此URL衍生自您在* Federation service name*欄位中輸入的值。



2. 選取連結、或複製URL並貼到瀏覽器、以存取身分識別供應商的登入頁面。
3. 若要確認您可以使用SSO登入StorageGRID 支援功能、請選取*登入下列其中一個站台*、選取您主要管理節點的依賴方識別碼、然後選取*登入*。

4. 輸入您的聯盟使用者名稱和密碼。
   - 如果SSO登入和登出作業成功、就會出現成功訊息。



   - 如果SSO作業不成功、會出現錯誤訊息。請修正問題、清除瀏覽器的Cookie、然後再試一次。
5. 重複這些步驟、驗證網格中每個管理節點的SSO連線。

Azure

步驟

1. 前往Azure入口網站的「單一登入」頁面。
2. 選擇*測試此應用程式*。
3. 輸入同盟使用者的認證資料。
   - 如果SSO登入和登出作業成功、就會出現成功訊息。

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

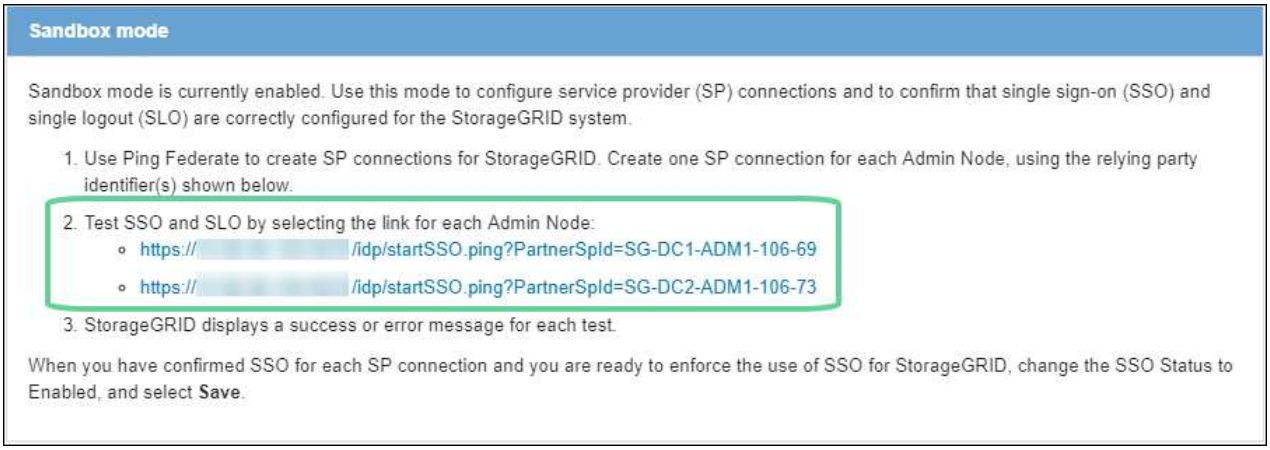
   - 如果SSO作業不成功、會出現錯誤訊息。請修正問題、清除瀏覽器的Cookie、然後再試一次。
4. 重複這些步驟、驗證網格中每個管理節點的SSO連線。

PingFedate

步驟

1. 從「功能表單一登入」頁面、選取沙箱模式訊息中的第一個連結。StorageGRID

   一次選取並測試一個連結。



2. 輸入同盟使用者的認證資料。
   - 如果SSO登入和登出作業成功、就會出現成功訊息。

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

   - 如果SSO作業不成功、會出現錯誤訊息。請修正問題、清除瀏覽器的Cookie、然後再試一次。
3. 選取下一個連結、驗證網格中每個管理節點的SSO連線。

   如果您看到「頁面過期」訊息、請在瀏覽器中選取「上一步」按鈕、然後重新提交認證資料。

啟用單一登入

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

啟用SSO時、所有使用者都必須使用SSO存取Grid Manager、租戶管理程式、Grid Management API及租戶管理API。本機使用者無法再存取StorageGRID 此功能。

步驟

1. 選擇*組態*>*存取控制*>*單一登入*。
2. 將SSO狀態變更為*已啟用*。
3. 選擇*保存*。
4. 檢閱警告訊息、然後選取*確定*。

   現在已啟用單一登入。

如果您使用Azure Portal、並StorageGRID 從用來存取Azure的同一部電腦存取驗證、請確定Azure Portal使用者也是授權StorageGRID 的使用者（已匯入StorageGRID 到「驗證」的聯盟群組中的使用者）。 或登出Azure Portal後再嘗試登入StorageGRID 。

在**AD FS**中建立依賴方信任

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關係人信任。您可以使用PowerShell命令、從StorageGRID 支援中心匯入SAML中繼資料、或手動輸入資料、來建立依賴方信任。

開始之前

- 您已設定StorageGRID 單一登入以供使用、並選擇* AD FS*作為SSO類型。
- 在**Grid Manager**的「單一登入」頁面上選取「沙箱模式」。請參閱 "使用沙箱模式"。
- 您知道系統中每個管理節點的完整網域名稱（或IP位址）和依賴方識別碼。您可以在StorageGRID 「管理員節點詳細資料」表的「單個登入」頁面上找到這些值。

  您必須為StorageGRID 您的系統中的每個管理節點建立信賴關係人信任關係。信任每個管理節點的依賴方、可確保使用者能夠安全地登入及登出任何管理節點。

- 您有在AD FS中建立信賴關係人信任關係的經驗、或是可以存取Microsoft AD FS文件。
- 您使用的是AD FS管理嵌入式管理單元、屬於「系統管理員」群組。
- 如果您是手動建立信賴關係人信任關係、則您擁有上傳至StorageGRID 該管理介面的自訂憑證、或者您知道如何從命令Shell登入管理節點。

關於這項工作

這些指示適用於Windows Server 2016 AD FS。如果您使用的是不同版本的AD FS、您會注意到程序上的細微差異。如有任何問題、請參閱Microsoft AD FS文件。

使用**Windows PowerShell**建立信賴廠商信任

您可以使用Windows PowerShell快速建立一或多個信賴關係人信任。

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命令提示字元中輸入下列命令：

   「Add-AdfsRelyingPartyTrust -Name「admin_Node_Identer」-Metadata URL "https://Admin_Node_FQDN/api/saml-metadata"

   - 適用於 `Admin_Node_Identifier`下、輸入管理節點的信賴方識別碼、完全如同「單一登入」頁面所示。例如、 `SG-DC1-ADM1`。
   - 適用於 `Admin_Node_FQDN`下、輸入相同管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）
3. 從Windows Server Manager中、選取* Tools **>** AD FS Management *。

   隨即顯示AD FS管理工具。
4. 選取「* AD FS*>*信賴廠商信任*」。

   此時會出現信賴方信任清單。
5. 新增存取控制原則至新建立的信賴關係人信任：
   a. 找出您剛建立的信賴關係人。
   b. 在信任上按一下滑鼠右鍵、然後選取*編輯存取控制原則*。
   c. 選取存取控制原則。
   d. 選取*「Apply」（套用）、然後選取「OK」（確定）*
6. 新增請款核發政策至新建立的信賴方信託：
   a. 找出您剛建立的信賴關係人。
   b. 以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。
   c. 選取*新增規則*。
   d. 在Select Rule Template（選擇規則範本）頁面上、從清單中選取* Send LDAP Attributes*（將LDAP屬性傳送為請款）、然後選取* Next*（下一步*）。
   e. 在「設定規則」頁面上、輸入此規則的顯示名稱。

      例如，* 對象 GUID 至名稱 ID* 或 * UPN 至名稱 ID* 。
   f. 針對屬性存放區、選取* Active Directory *。
   g. 在「對應」表格的 LDAP 屬性欄中、輸入 * objectGUID* 或選取 * 使用者主體名稱 * 。
   h. 在「對應」表格的「傳出請款類型」欄中、從下拉式清單中選取*名稱ID*。
   i. 選擇*完成*、然後選擇*確定*。
7. 確認中繼資料已成功匯入。
   a. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。
   b. 確認已填入*端點*、*識別項*和*簽名*索引標籤上的欄位。

如果中繼資料遺失、請確認同盟中繼資料位址正確、或手動輸入值。

8. 重複這些步驟、為StorageGRID 您的整套系統中的所有管理節點設定依賴方信任。
9. 完成後、請返回StorageGRID 「還原」並測試所有信賴關係人的信任、以確認其設定正確。請參閱 "使用沙箱模式" 以取得相關指示。

透過匯入聯盟中繼資料來建立依賴方信任

您可以存取每個管理節點的SAML中繼資料、以匯入每個信賴方信任的值。

步驟

1. 在Windows Server Manager中、選取*工具*、然後選取* AD FS管理*。
2. 在「Actions（動作）」下、選取「* Add S依賴 方Trust（*新增信賴方
3. 在歡迎頁面上、選擇* Claims感知*、然後選取* Start*。
4. 選取*匯入線上發佈的依賴方相關資料、或是本機網路上的相關資料*。
5. 在*聯盟中繼資料位址（主機名稱或URL）*中、輸入此管理節點的SAML中繼資料位置：

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

   適用於 `Admin_Node_FQDN` 下、輸入相同管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）

6. 完成「信賴方信任」精靈、儲存信賴方信任、然後關閉精靈。

   輸入顯示名稱時、請使用管理節點的信賴方識別碼、如同網格管理器的「單一登入」頁面上所顯示的一樣。例如、 `SG-DC1-ADM1`。

7. 新增報銷規則：
   a. 以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。
   b. 選擇*新增規則*：
   c. 在Select Rule Template（選擇規則範本）頁面上、從清單中選取* Send LDAP Attributes*（將LDAP屬性傳送為請款）、然後選取* Next*（下一步*）。
   d. 在「設定規則」頁面上、輸入此規則的顯示名稱。

      例如，* 對象 GUID 至名稱 ID* 或 * UPN 至名稱 ID* 。

   e. 針對屬性存放區、選取* Active Directory *。
   f. 在「對應」表格的 LDAP 屬性欄中、輸入 * objectGUID* 或選取 * 使用者主體名稱 * 。
   g. 在「對應」表格的「傳出請款類型」欄中、從下拉式清單中選取*名稱ID*。
   h. 選擇*完成*、然後選擇*確定*。
8. 確認中繼資料已成功匯入。
   a. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。
   b. 確認已填入*端點*、*識別項*和*簽名*索引標籤上的欄位。

如果中繼資料遺失、請確認同盟中繼資料位址正確、或手動輸入值。

9. 重複這些步驟、為StorageGRID 您的整套系統中的所有管理節點設定依賴方信任。
10. 完成後、請返回StorageGRID 「還原」並測試所有信賴關係人的信任、以確認其設定正確。請參閱 "使用沙箱模式" 以取得相關指示。

手動建立依賴方信任

如果您選擇不匯入依賴零件信任的資料、您可以手動輸入值。

步驟

1. 在Windows Server Manager中、選取*工具*、然後選取* AD FS管理*。
2. 在「Actions（動作）」下、選取「* Add S依賴 方Trust（*新增信賴方
3. 在歡迎頁面上、選擇* Claims感知*、然後選取* Start*。
4. 選取*手動輸入依賴方的相關資料*、然後選取*下一步*。
5. 完成信賴廠商信任精靈：

   a. 輸入此管理節點的顯示名稱。

      為確保一致性、請使用管理節點的信賴方識別碼、如同網格管理器的「單一登入」頁面上所顯示的一樣。例如、 `SG-DC1-ADM1`。

   b. 跳過設定選用權杖加密憑證的步驟。

   c. 在「設定 URL 」頁面上、選取 * 啟用 SAML 2.0 WebSSO 傳輸協定的支援 * 核取方塊。

   d. 輸入管理節點的SAML服務端點URL：

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

      適用於 `*Admin_Node_FQDN*`下、輸入管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）

   e. 在「設定識別碼」頁面上、指定相同管理節點的信賴方識別碼：

      `*Admin_Node_Identifier*`

      適用於 `*Admin_Node_Identifier*`下、輸入管理節點的信賴方識別碼、完全如同「單一登入」頁面所示。例如、 `SG-DC1-ADM1`。

   f. 檢閱設定、儲存信賴關係人信任、然後關閉精靈。

      此時會出現「編輯請款核發原則」對話方塊。

      如果對話方塊未出現、請以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。

6. 若要啟動「請款規則」精靈、請選取*「新增規則*」：

   a. 在Select Rule Template（選擇規則範本）頁面上、從清單中選取* Send LDAP Attributes*（將LDAP屬

性傳送為請款）、然後選取* Next*（下一步*）。

b. 在「設定規則」頁面上、輸入此規則的顯示名稱。

例如，* 對象 GUID 至名稱 ID* 或 * UPN 至名稱 ID* 。

c. 針對屬性存放區、選取* Active Directory *。

d. 在「對應」表格的 LDAP 屬性欄中、輸入 * objectGUID* 或選取 * 使用者主體名稱 * 。

e. 在「對應」表格的「傳出請款類型」欄中、從下拉式清單中選取*名稱ID*。

f. 選擇*完成*、然後選擇*確定*。

7. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。

8. 在「端點」索引標籤上、設定單一登出（SLO）的端點：

a. 選擇* Add SAML（添加SAML）*。

b. 選擇*端點類型*>* SAML登出*。

c. 選擇* Binding（綁定）* **Redirect**（重定向*）。

d. 在「信任的**URL**」欄位中、輸入此管理節點用於單一登出（SLO）的URL：

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

適用於 `*Admin_Node_FQDN*` 下、輸入管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）

a. 選擇*確定*。

9. 在*簽名*索引標籤上、指定此信賴憑證方信任的簽名證書：

a. 新增自訂憑證：

- 如果您有上傳至StorageGRID 該功能的自訂管理憑證、請選取該憑證。
- 如果您沒有自訂憑證、請登入管理節點、前往 `/var/local/mgmt-api` 管理節點的目錄、然後新增 `custom-server.crt` 憑證檔案：

*附註：*使用管理節點的預設憑證 (`server.crt`）不建議使用。如果管理節點故障、當您恢復節點時、將會重新產生預設憑證、您將需要更新依賴方信任。

b. 選取*「Apply」（套用）、然後選取「OK」（確定）*。

依賴方屬性會儲存並關閉。

10. 重複這些步驟、為StorageGRID 您的整套系統中的所有管理節點設定依賴方信任。

11. 完成後、請返回StorageGRID 「還原」並測試所有信賴關係人的信任、以確認其設定正確。請參閱 "使用沙箱模式" 以取得相關指示。

在**Azure AD**中建立企業應用程式

您可以使用Azure AD為系統中的每個管理節點建立企業應用程式。

開始之前

- 您已開始設定StorageGRID 單一登入功能以供使用、並選擇* Azure *作為SSO類型。
- 在**Grid Manager**的「單一登入」頁面上選取「沙箱模式」。請參閱 "使用沙箱模式"。
- 您的系統中每個管理節點都有*企業應用程式名稱*。您可以從StorageGRID 「管理員節點」詳細資料表中複製這些值、該表位於「報價單一登入」頁面。

> 您必須為StorageGRID 您的系統中的每個管理節點建立企業應用程式。為每個管理節點設定企業應用程式、可確保使用者安全地登入及登出任何管理節點。

- 您有在Azure Active Directory中建立企業應用程式的經驗。
- 您有一個Azure帳戶、且有有效的訂閱。
- 您在Azure帳戶中有下列任一角色：Global Administrator、Cloud Application Administrator、Application Administrator或服務主體的擁有者。

存取**Azure AD**

步驟

1. 登入 "Azure Portal"。
2. 瀏覽至 "Azure Active Directory"。
3. 選取 "企業應用程式"。

建立企業應用程式並儲存**StorageGRID** 不可靠的**SSO**組態

若要在 StorageGRID 中儲存 Azure 的 SSO 組態、您必須使用 Azure 為每個管理節點建立企業應用程式。您將從Azure複製聯盟中繼資料URL、然後貼到StorageGRID 「支援單一登入」頁面上對應的*聯盟中繼資料URL*欄位。

步驟

1. 針對每個管理節點重複下列步驟。
   a. 在Azure Enterprise應用程式窗格中、選取*新增應用程式*。
   b. 選取*建立您自己的應用程式*。
   c. 如需名稱、請在StorageGRID 「Data Name（管理員節點）」詳細資料表中輸入您複製的*企業應用程式名稱*（英文）、位於「Data Flash（英文）」頁面上。
   d. 選擇*整合您在圖庫中找不到的任何其他應用程式（非圖庫）*選項按鈕。
   e. 選擇* Create （建立）。
   f. 選取* 2中的*入門*連結。設定單一登入*方塊、或選取左邊界的*單一登入*連結。
   g. 選取「* SAML *」方塊。
   h. 複製*應用程式聯盟中繼資料URL*、可在*步驟3 SAML簽署憑證*下找到。
   i. 前往StorageGRID 「僅供參考的單一登入」頁面、然後將URL貼到*聯盟中繼資料URL*欄位、此欄位對應您使用的*企業應用程式名稱*。
2. 在貼上每個管理節點的聯盟中繼資料URL、並對SSO組態進行所有其他必要變更之後、請在StorageGRID 「支援單一登入」頁面上選取「儲存」。

下載每個管理節點的**SAML**中繼資料

儲存SSO組態之後、您可以為StorageGRID 您的系統中的每個管理節點下載SAML中繼資料檔案。

步驟

1. 針對每個管理節點重複這些步驟。
   a. 從管理節點登入StorageGRID 到這個功能。
   b. 選擇*組態*>*存取控制*>*單一登入*。
   c. 選取按鈕、即可下載該管理節點的SAML中繼資料。
   d. 儲存您要上傳至Azure AD的檔案。

將**SAML**中繼資料上傳至每個企業應用程式

下載每StorageGRID 個「支援對象管理節點」的SAML中繼資料檔案之後、請在Azure AD中執行下列步驟：

步驟

1. 返回Azure Portal。
2. 針對每個企業應用程式重複這些步驟：

   您可能需要重新整理「企業應用程式」頁面、以查看先前新增至清單中的應用程式。

   a. 前往企業應用程式的「內容」頁面。
   b. 將*需要指派*設為*否*（除非您要個別設定指派）。
   c. 前往單一登入頁面。
   d. 完成SAML組態。
   e. 選取*上傳中繼資料檔案*按鈕、然後選取您為對應的管理節點下載的SAML中繼資料檔案。
   f. 載入檔案後、選取*「Save"（儲存）、然後選取「 X*」以關閉窗格。您將返回「使用SAML設定單一登入」頁面。
3. 請依照中的步驟進行 "使用沙箱模式" 測試每個應用程式。

在**PingFedate**中建立服務供應商（**SP**）連線

您可以使用PingFedate為系統中的每個管理節點建立服務供應商（SP）連線。為了加速程序、您將從StorageGRID S倚賴 者處匯入SAML中繼資料。

開始之前

- 您已設定StorageGRID 單一登入以供使用、並選擇* Ping federate*作為SSO類型。
- 在**Grid Manager**的「單一登入」頁面上選取「沙箱模式」。請參閱 "使用沙箱模式"。
- 您的系統中每個管理節點都有* SP連線ID*。您可以在StorageGRID 「管理員節點詳細資料」表的「單個登入」頁面上找到這些值。
- 您已下載系統中每個管理節點的* SAML中繼資料*。
- 您在PingFedate伺服器上建立SP連線的經驗豐富。

- 您擁有 "系統管理員參考指南" 適用於PingFedate伺服器。PingFedate文件提供詳細的逐步指示和說明。
- 您擁有 "管理員權限" 適用於PingFedate伺服器。

關於這項工作

以下說明概述如何將PingFedate Server版本10.3設定為StorageGRID SSO供應商以供支援。如果您使用的是另一個版本的PingFedate、您可能需要調整這些指示。請參閱PingFedate伺服器文件、以取得版本的詳細指示。

完整的**PingFedate**必備條件

在建立要用於StorageGRID 觀賞的SP連線之前、您必須先在PingFederate完成必要的工作。設定SP連線時、您將會使用這些必要條件的資訊。

建立資料儲存區**[data-store]**

如果您尚未建立資料存放區、請建立資料存放區、將PingFedate連線至AD FS LDAP伺服器。使用您使用的值 "設定身分識別聯盟" 在StorageGRID

- 類型：目錄（LDAP）
- * LDAP類型*：Active Directory
- 二進位屬性名稱：在LDAP二進位屬性索引標籤上輸入* objectGUID*、完全如圖所示。

建立密碼認證驗證器[密碼 驗證器]

如果您還沒有、請建立密碼認證驗證程式。

- 類型：LDAP使用者名稱密碼認證驗證程式
- 資料儲存區：選取您建立的資料儲存區。
- 搜尋基礎：輸入LDAP的資訊（例如：DC=SAML、DC=sgws）。
- 搜尋篩選器：SamAccountName=${userName}
- 範圍：子樹狀結構

建立**IDP**介面卡執行個體**[[**介 面卡執行個體**]**

如果您尚未建立IDP介面卡執行個體、請建立一個IDP介面卡執行個體。

步驟

1. 轉至*驗證*>*整合*>* IDP介面卡*。
2. 選擇* Create New Instance*（創建新實例*）。
3. 在類型索引標籤上、選取* HTML表單IDP介面卡*。
4. 在IDP介面卡索引標籤上、選取*新增一列至「認證驗證程式」*。
5. 選取 密碼認證驗證工具 您已建立。
6. 在Adapter Attributes*（適配器屬性）選項卡上，選擇* pseudonyation*的* username*屬性。
7. 選擇*保存*。

建立或匯入簽署憑證[[Signing認證證]

如果您尚未建立簽署憑證、請建立或匯入簽署憑證。

步驟

1. 請前往*安全*>*簽署與解密金鑰與憑證*。
2. 建立或匯入簽署憑證。

在PingFedate建立SP連線

當您在PingFedate建立SP連線時、會將從StorageGRID 支援管理節點的支援節點下載的SAML中繼資料匯入。中繼資料檔案包含許多您需要的特定值。

> 您必須為StorageGRID 您的支援系統中的每個管理節點建立SP連線、以便使用者安全地登入和登出任何節點。請依照下列指示建立第一個SP連線。然後前往 建立其他SP連線 建立所需的任何其他連線。

選擇SP連線類型

步驟

1. 請參訪*應用程式*>*整合*>* SP連線*。
2. 選取*建立連線*。
3. 選擇*不要使用範本進行此連線*。
4. 選擇*瀏覽器SSO設定檔*和* SAML 2.0*作為傳輸協定。

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. 從StorageGRID 「管理節點的「支援單一登入」頁面下載的SAML中繼資料檔案。
3. 檢閱中繼資料摘要和一般資訊索引標籤上提供的資訊。

   合作夥伴的實體ID和連線名稱均設定StorageGRID 為整套SP連線ID。（例如10.96105.200-DC1-ADM1-105-200）。基礎URL是StorageGRID 指「物件管理節點」的IP。

4. 選擇*下一步*。

設定IDP瀏覽器SSO

步驟

1. 從瀏覽器SSO索引標籤、選取*設定瀏覽器SSSSO *。
2. 在「SAML設定檔」索引標籤上、選取「* SP啟動的SSO*」、「* SP初始SLO*」、「* IDP啟動的SSO*」和「* IDP啟動的SLO*」選項。
3. 選擇*下一步*。
4. 在Assertion壽命索引標籤上、不做任何變更。
5. 在Assertion Creation（聲明創建）選項卡上，選擇* Configure Assertion creation （配置聲明創建）。

a. 在「身分識別對應」索引標籤上、選取「標準」。

b. 在「屬性合約」索引標籤上、使用* SAML Subject *做為「屬性合約」、以及匯入的未指定名稱格式。

6. 若要延長合約、請選取 * 刪除 * 以移除 `urn:oid`，不使用。

對應介面卡執行個體

步驟

1. 在驗證來源對應索引標籤上、選取*對應新介面卡執行個體*。
2. 在介面卡執行個體索引標籤上、選取 介面卡執行個體 您已建立。
3. 在「對應方法」索引標籤上、選取*從資料儲存區擷取其他屬性*。
4. 在「屬性來源與使用者查詢」索引標籤上、選取「新增屬性來源」。
5. 在「Data Store（資料儲存區）」索引標籤上、提供說明並選取 資料儲存區 您已新增。
6. 在LDAP目錄搜尋索引標籤上：
   - 輸入*基礎DN*、此DN應與StorageGRID 您在知識庫中輸入的LDAP伺服器值完全相符。
   - 在搜尋範圍中、選取* Subtree *。
   - 對於根物件類別、請搜尋並新增下列其中一個屬性： * 物件 GUID* 或 * userPrincipalName* 。
7. 在LDAP二進位屬性編碼類型索引標籤上、針對* objectGUID*屬性選取* Base64*。
8. 在LDAP Filter（LDAP篩選器）索引標籤上、輸入* sAMAccountName=${userName} *。
9. 在「屬性合約履行」標籤上、從「來源」下拉式清單中選取 * LDAP （屬性） * 、然後從「值」下拉式清單中選取 * objectGUID* 或 * userPrincipalName* 。
10. 檢閱並儲存屬性來源。
11. 在「故障儲存屬性來源」索引標籤上、選取*中止SSO交易*。
12. 檢閱摘要、然後選取*「完成」*。
13. 選擇*完成*。

設定傳輸協定設定

步驟

1. 在* SP Connection*>*瀏覽器SSSSO >*傳輸協定設定*索引標籤上、選取*設定傳輸協定設定。
2. 在 Assertion Consumer Service URL 標籤上、接受從 StorageGRID SAML 中繼資料（ * POST * for Binding and ）匯入的預設值 `/api/saml-response` 端點 URL ）。
3. 在「 SLO 服務 URL 」標籤上、接受從 StorageGRID SAML 中繼資料匯入的預設值（ * 重新導向 * 用於連結和 `/api/saml-logout` 端點 URL 。
4. 在允許的 SAML 繫結標籤上、清除 * 成品 * 和 * SOAP* 。只需要* POST 和*重新導向。
5. 在「簽章原則」索引標籤上、保留「 * 需要簽署驗證要求 * 」和「 * 永遠簽署聲明 * 」核取方塊的核取方塊。
6. 在加密原則索引標籤上、選取*無*。
7. 檢閱摘要並選取*完成*以儲存傳輸協定設定。
8. 檢閱摘要並選取*完成*以儲存瀏覽器SSO設定。

設定認證資料

步驟

1. 從SP連線索引標籤、選取*認證*。
2. 從「認證」標籤中、選取*「設定認證」*。
3. 選取 簽署憑證 您已建立或匯入。
4. 選擇*下一步*以前往*管理簽名驗證設定*。
   a. 在信任模式索引標籤上、選取*未鎖定*。
   b. 在「簽名驗證憑證」索引標籤上、檢閱從StorageGRID 「支援SAML」中繼資料匯入的簽署憑證資訊。
5. 檢閱摘要畫面、然後選取*「Save"（儲存）以儲存SP連線。

建立其他**SP**連線

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。您上傳每個複本的新中繼資料。

不同管理節點的SP連線使用相同的設定、但合作夥伴的實體ID、基礎URL、連線ID、連線名稱、簽名驗證、 和SLO回應URL。

步驟

1. 選擇* Action">* Copy*、為每個額外的管理節點建立初始SP連線的複本。
2. 輸入複本的「連線ID」和「連線名稱」、然後選取*「儲存*」。
3. 選擇對應至管理節點的中繼資料檔案：
   a. 選擇* Action">* Update with中繼資料*。
   b. 選擇*選擇「檔案」*並上傳中繼資料。
   c. 選擇*下一步*。
   d. 選擇*保存*。
4. 解決由於未使用屬性而導致的錯誤：
   a. 選取新連線。
   b. 選取*設定瀏覽器SSO >設定宣告建立>屬性合約*。
   c. 刪除* urn:OID*的項目。
   d. 選擇*保存*。

停用單一登入

如果您不想再使用此功能、可以停用單一登入（SSO）。您必須先停用單一登入、才能停用身分識別聯盟。

開始之前

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

步驟

1. 選擇*組態*>*存取控制*>*單一登入*。

   此時會出現「單一登入」頁面。

2. 選取*停用*選項。
3. 選擇*保存*。

   此時會出現一則警告訊息、指出本機使用者現在可以登入。

4. 選擇*確定*。

   下次登入StorageGRID 時StorageGRID 、會出現「畫面上顯示「資訊區登入」頁面、您必須輸入本機StorageGRID 或聯盟使用者的使用者名稱和密碼。

暫時停用並重新啟用單一管理節點的單一登入

如果單一登入（SSO）系統當機、您可能無法登入Grid Manager。在此情況下、您可以暫時停用及重新啟用單一管理節點的SSO。若要停用及重新啟用SSO、您必須存取節點的命令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。

關於這項工作

停用單一管理節點的SSO之後、您可以以本機根使用者的身分登入Grid Manager。若要保護StorageGRID 您的不穩定系統、您必須在登出時、使用節點的命令Shell在管理節點上重新啟用SSO。

停用單一管理節點的SSO並不會影響網格中任何其他管理節點的SSO設定。Grid Manager 中「單一登入」頁面上的「啟用 SSO 」核取方塊會保持選取狀態、除非您更新現有的 SSO 設定、否則所有的 SSO 設定都會保留。

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。

2. 執行下列命令：`disable-saml`

訊息表示該命令僅適用於此管理節點。

3. 確認您要停用SSO。

   訊息表示節點上的單一登入已停用。

4. 從網頁瀏覽器存取同一個管理節點上的Grid Manager。

   現在會顯示Grid Manager登入頁面、因為SSO已停用。

5. 使用root使用者名稱和本機root使用者密碼登入。
6. 如果您因為需要修正SSO組態而暫時停用SSO：
   a. 選擇*組態*>*存取控制*>*單一登入*。
   b. 變更不正確或過時的SSO設定。
   c. 選擇*保存*。

      從「單一登入」頁面選取「儲存」、會自動重新啟用整個網格的SSO功能。

7. 如果您因為其他原因而需要存取Grid Manager而暫時停用SSO：
   a. 執行您需要執行的任何工作或工作。
   b. 選取 * 登出 * 、然後關閉 Grid Manager 。
   c. 在管理節點上重新啟用SSO。您可以執行下列任一步驟：

      - 執行下列命令： `enable-saml`

        訊息表示該命令僅適用於此管理節點。

      確認您要啟用SSO。

   訊息表示節點上已啟用單一登入。

   - 重新開機網格節點： `reboot`

8. 從網頁瀏覽器、從相同的管理節點存取Grid Manager。
9. 確認StorageGRID 畫面出現「畫面不顯示登入」頁面、且您必須輸入SSO認證、才能存取Grid Manager。