



# 使用單一登入 (SSO)

## StorageGRID software

NetApp  
May 29, 2026

# 目錄

使用單一登入 (SSO)	1
配置單一登入	1
單一登入的工作原理	1
單一登入的要求和注意事項	3
身份提供者要求	4
伺服器證書要求	4
端口要求	5
確認聯合用戶可以登入	5
使用沙盒模式	6
訪問沙盒模式	7
輸入身份提供者詳細信息	8
配置信賴方信任、企業應用程式或SP連接	11
測試 SSO 連接	12
啟用單一登入	14
在 AD FS 中創造信賴方信任	15
使用 Windows PowerShell 建立信賴方信任	15
透過匯入聯合元資料創建信賴方信任	17
手動創建信賴方信任	18
在 Azure AD 中建立企業應用程式	19
存取 Azure AD	20
建立企業應用程式並儲存StorageGRID SSO 配置	20
下載每個管理節點的 SAML 元數據	21
將 SAML 元資料上傳到每個企業應用程式	21
在 PingFederate 中建立服務提供者 (SP) 連接	21
完成 PingFederate 中的先決條件	22
在 PingFederate 中建立SP連接	23
停用單一登入	25
暫時停用並重新啟用一個管理節點的單一登入	26

# 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

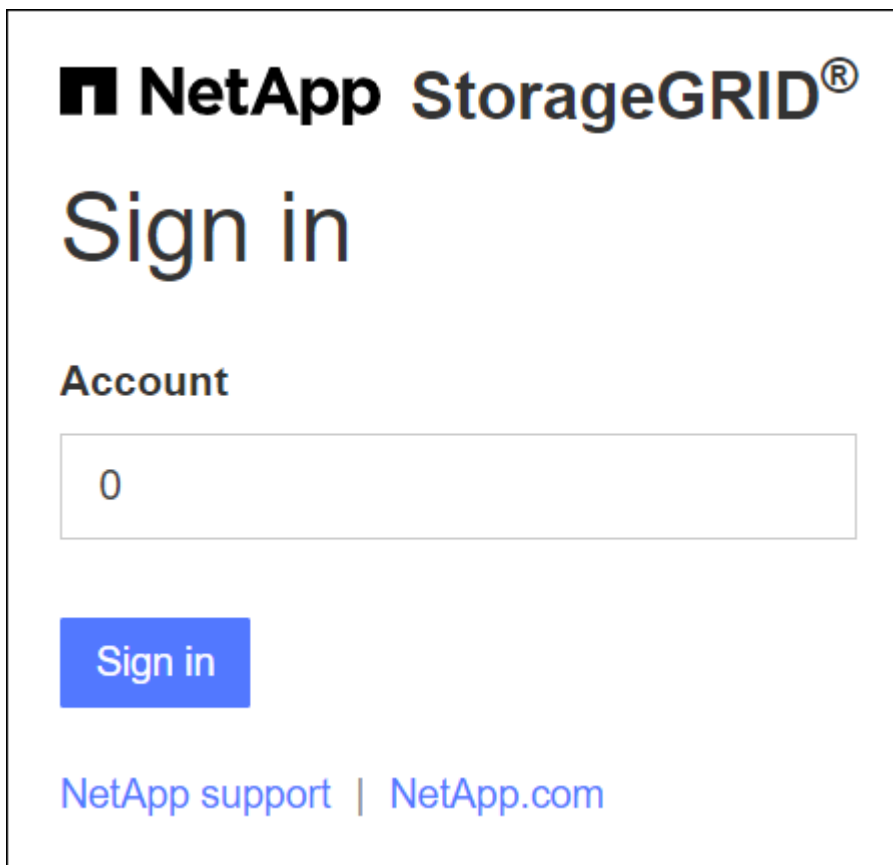
當啟用 SSO 並且您登入 StorageGRID 時，您將被重新導向到您組織的 SSO 頁面以驗證您的憑證。

#### 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 StorageGRID Sign 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：



**NetApp StorageGRID®**

# Sign in

**Account**

[Sign in](#)

[NetApp support](#) | [NetApp.com](#)

- 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：



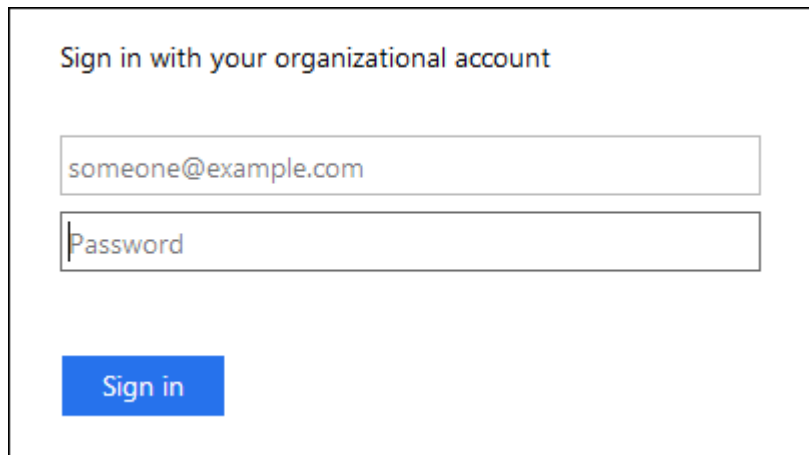
當您 Sign in 租用戶帳戶的完整 URL（即完全限定網域名稱或 IP 位址，後面接著 `/?accountId=20-digit-account-id`）。相反，您會立即重定向到您組織的 SSO 登入頁面，您可以在其中 [使用您的 SSO 憑證登入](#)。

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	<ul style="list-style-type: none"><li>• 活動目錄</li><li>• Azure</li><li>• Ping聯邦</li></ul>
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

受限的網絡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絡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

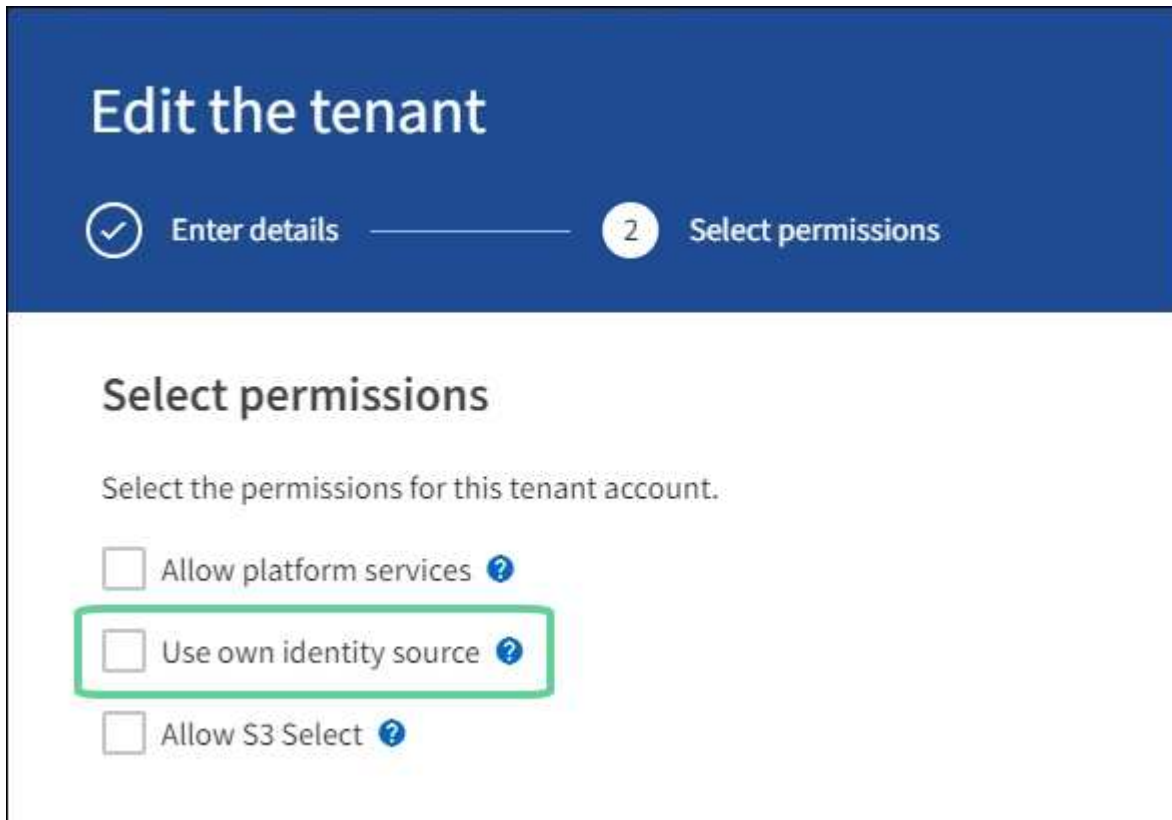
1. 如果存在現有租用戶帳戶，請確認沒有任何租戶使用其自己的身分來源。



啟用 SSO 時，租用戶管理員中設定的身份來源將會被網絡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絡管理器：
    - a. 從網絡管理員中，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絡管理器。
  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. 從網絡管理器中選擇\*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	<ul style="list-style-type: none"> <li>• 活動目錄</li> <li>• Azure</li> <li>• Ping聯邦</li> </ul>
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 身分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。

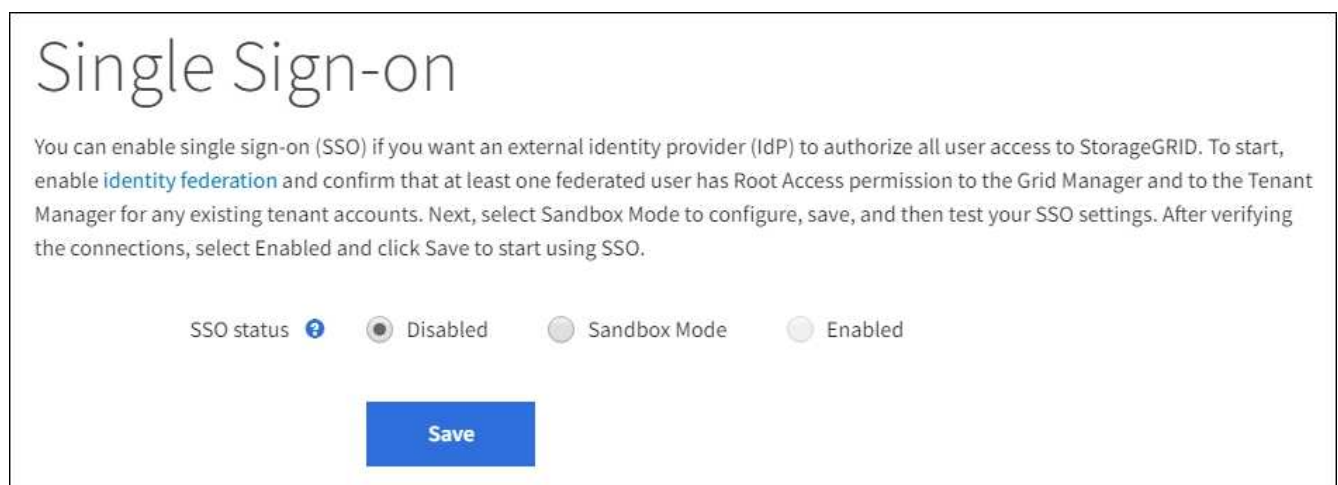
沙盒模式可以輕鬆執行此來回配置，並在啟用 SSO 之前測試所有設定。當您使用沙盒模式時，使用者無法使用 SSO 登入。

## 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 進入網絡管理器。

- 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，如果您的網絡只有一個管理節點，且您不打算在將來新增更多管理節點，請輸入 SG` 或者 `StorageGRID。
- 如果您的網絡包含多個管理節點，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。

Save ✓

## 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。

#### Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

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**。

You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

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。

✔ 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。

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。

**Sandbox mode**

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
  - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
  - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

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_Identifier" -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。
- 在網絡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](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StorageGRIDSigin 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，您可能無法登入網絡管理員。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 使用者身分登入網絡管理員。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 不會影響網絡中任何其他管理節點的 SSO 設定。網絡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 StorageGRID Sign in 頁面，並且您必須輸入 SSO 憑證才能存取網格管理員。

## 版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

## 商標資訊

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