



使用單一登入 (SSO) StorageGRID 進行支援 StorageGRID 11.5

NetApp
April 11, 2024

目錄

使用單一登入 (SSO) StorageGRID 進行支援	1
單一登入的運作方式	1
使用單一登入的需求	3
設定單一登入	4

使用單一登入（SSO） StorageGRID 進行支援

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。啟用SSO時、所有使用者必須先經過外部身分識別供應商的驗證、才能存取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到無法使用的功能。

- "單一登入的運作方式"
- "使用單一登入的需求"
- "設定單一登入"

單一登入的運作方式

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

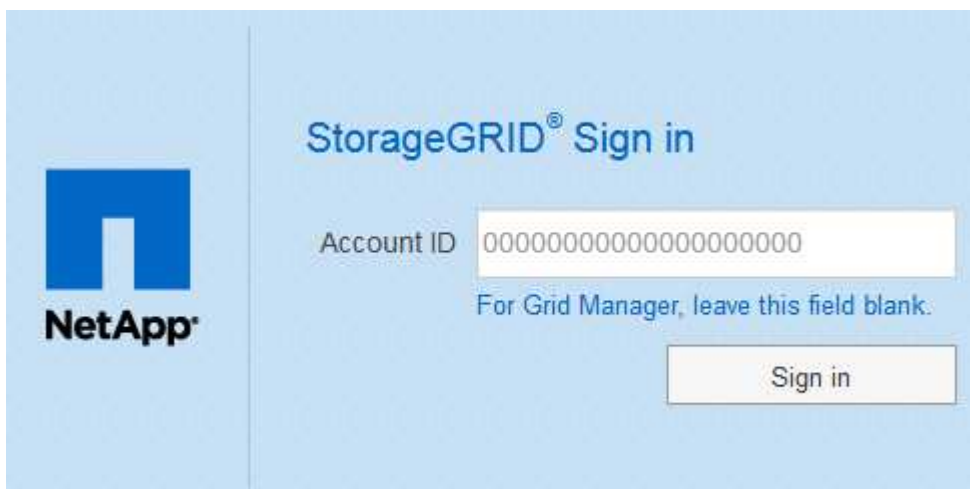
啟用SSO並登入StorageGRID 支援功能時、系統會將您重新導向至組織的SSO頁面、以驗證您的認證資料。

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：

A screenshot of the StorageGRID Sign in page. On the left is the NetApp logo. The main content area has the title "StorageGRID® Sign in". Below the title is a form with a label "Account ID" and a text input field containing "00000000000000000000". Below the input field is the text "For Grid Manager, leave this field blank." At the bottom right of the form is a "Sign in" button.

- 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：



The image shows the StorageGRID Sign in interface. On the left is the NetApp logo. The main area is titled 'StorageGRID® Sign in'. It features a 'Recent' dropdown menu with 'S3 tenant' selected. Below it is an 'Account ID' text input field containing '27469746059057031822'. A note below the field says 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.



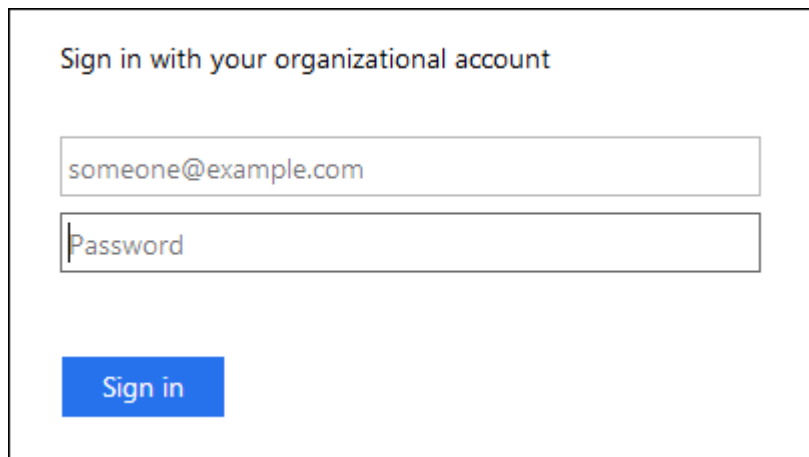
輸入租戶帳戶的完整URL（即完整網域名稱或IP位址之後）時、不會顯示「協助登入」頁面StorageGRID /?accountId=20-digit-account-id）。而是會立即重新導向至組織的SSO登入頁面、您可以在其中登入 [使用SSO認證登入](#)。

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. 按一下*登入*

可將您重新導向至組織的SSO登入頁面。StorageGRID例如：



The image shows a sign-in form titled 'Sign in with your organizational account'. It has two input fields: the first contains 'someone@example.com' and the second is labeled 'Password'. Below the fields is a blue 'Sign in' button.

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、且您屬於具有足夠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。

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. 在使用者介面的右上角找到*登出*連結。
2. 按一下*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
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。

使用單一登入的需求

在啟用StorageGRID 適用於某個作業系統的單一登入（SSO）之前、請先檢閱本節的要求。



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）。

身分識別供應商要求

SSO的身分識別供應商（IDP）必須符合下列要求：

- 下列任一版本的Active Directory Federation Service（AD FS）：
 - Windows Server 2016隨附的AD FS 4.0



Windows Server 2016應該使用 "[KB3201845更新](#)"或更高版本。

- Windows Server 2012 R2更新或更新版本隨附的AD FS 3.0。
- 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

伺服器憑證需求

在每個管理節點上使用管理介面伺服器憑證、以安全存取Grid Manager、租戶管理程式、Grid Management API及租戶管理API StorageGRID。當您在StorageGRID AD FS中設定SSO依賴方信任功能時、您可以使用伺服器憑證做為簽署憑證、以利StorageGRID向AD FS提出要求。

如果您尚未為管理介面安裝自訂伺服器憑證、請立即安裝。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所有依賴方信任的情況下使用。



不建議在AD FS信賴方信任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AD FS中的依賴方信任。

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`。

相關資訊

["透過防火牆控制存取"](#)

["為Grid Manager和Tenant Manager設定自訂伺服器憑證"](#)

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。

- ["確認同盟使用者可以登入"](#)
- ["使用沙箱模式"](#)
- ["在AD FS中建立依賴方信任"](#)
- ["測試依賴方信任"](#)
- ["啟用單一登入"](#)
- ["停用單一登入"](#)
- ["暫時停用及重新啟用單一管理節點的單一登入"](#)

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。

您需要的產品

- 您必須使用支援的瀏覽器登入Grid Manager。

- 您必須擁有特定的存取權限。
- 您使用Active Directory做為聯盟身分識別來源、使用AD FS做為身分識別提供者。

"使用單一登入的需求"

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*存取控制*>*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、請確認不再需要任何可能用於此租戶帳戶的聯盟群組、取消選取核取方塊、然後按一下*「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、請確認具有「根存取」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、然後按一下*編輯帳戶*。
 - c. 如果選中了*使用自己的身份來源*複選框，請取消選中該複選框，然後單擊*保存*。

Edit Tenant Account

Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional)

Cancel

Save

此時會出現「租戶帳戶」頁面。

- a. 選取租戶帳戶、按一下*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、按一下*存取控制*>*群組*。
- c. 請確定至少已指派Grid Manager中的一個同盟群組給此租戶的「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

["使用單一登入的需求"](#)

["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依賴方信任的Active Directory Federation Services (AD FS)、然後再為StorageGRID 非使用者強制執行單一登入 (SSO)。啟用SSO之後、您可以重新啟用沙箱模式、以設定或測試新的和現有的信賴關係人信任。重新啟用沙箱模式可暫時停用StorageGRID SSO功能以供使用者使用。

您需要的產品

- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須擁有特定的存取權限。

關於這項工作

啟用SSO且使用者嘗試登入管理節點時StorageGRID、Sin會將驗證要求傳送至AD FS。反過來、AD FS會將驗證回應傳回StorageGRID 至S還原、指出授權要求是否成功。對於成功的要求、回應會包含使用者的通用唯一識別碼 (UUID)。

若要讓StorageGRID 驗證 (服務供應商) 和AD FS (身分識別供應商) 能夠安全地就使用者驗證要求進行通訊、您必須在StorageGRID 效益分析中設定某些設定。接下來、您必須使用AD FS為每個管理節點建立信賴關係人信任。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。



強烈建議使用沙箱模式、但並非嚴格要求。如果您準備好在StorageGRID 將SSO設定為「支援」後立即建立AD FS信賴關係人信任關係、而且您不需要測試每個管理節點的SSO和單一登入 (SLO) 程序、按一下「已啟用」、輸入StorageGRID 「支援」設定、為AD FS中的每個管理節點建立信賴關係人信任、然後按一下「儲存」以啟用SSO。

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。

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Save



如果未顯示SSO狀態選項、請確認您已將Active Directory設定為聯盟身分識別來源。請參閱「使用單一登入的要求」。

2. 選取*沙箱模式*選項。

此時會顯示「身分識別提供者」和「信賴方」設定。在「身分識別提供者」區段中、「服務類型」欄位為唯讀。它會顯示您所使用的身分識別聯盟服務類型（例如Active Directory）。

3. 在「身分識別提供者」區段中：

- 輸入Federation Service名稱、完全如同AD FS中所示。



若要尋找Federation Service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。

- 指定當身分識別供應商傳送SSO組態資訊以回應StorageGRID 需求時、是否要使用傳輸層安全性（TLS）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。

如果您選取此設定、請複製並貼上「* CA認證*」文字方塊中的認證。

- 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

4. 在「依賴方」區段中、指定StorageGRID 當您設定依賴方信任時、將用於「管理員節點」的依賴方識別碼。

- 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、其中包含每個管理節點的依賴方識別碼。+附註：您必須為StorageGRID 您的支援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。

5. 按一下「* 儲存 *」。

- 「儲存」按鈕上會出現綠色勾號幾秒鐘。

Save



- 。此時會出現沙箱模式確認通知、確認沙箱模式已啟用。當您使用AD FS設定每個管理節點的依賴方信任、並測試單一登入（SSO）和單一登出（SLO）程序時、可以使用此模式。

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

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.

相關資訊

["使用單一登入的需求"](#)

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。

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。

您需要的產品

- 您已將SSO設定為StorageGRID「支援」、而且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。

關於這項工作

這些指示適用於Windows Server 2016隨附的AD FS 4.0。如果您使用的是Windows 2012 R2隨附的AD FS 3.0、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。

步驟

1. 在Windows開始功能表中、以滑鼠右鍵按一下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_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- 適用於 *Admin_Node_Identifer* 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. 按一下「套用」、然後按一下「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. 按一下*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）、然後按一下* 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、* ObjectGuid至Name 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*。
- 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. 按一下「完成」、然後按一下「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、或只是手動輸入值。

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 到「還原」和 "測試所有依賴方信任" 以確認設定正確。

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。

您需要的產品

- 您已將SSO設定為StorageGRID 「支援」、而且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。

關於這項工作

這些指示適用於Windows Server 2016隨附的AD FS 4.0。如果您使用的是Windows 2012 R2隨附的AD FS 3.0、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。

步驟

1. 在Windows Server Manager中、按一下*「工具」、然後選取「AD FS管理*」。
2. 在「Actions（動作）」下、按一下「* Add S依賴 方Trust (*新增
3. 在歡迎頁面上、選擇* Claims感知*、然後按一下*開始*。
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. 按一下*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）、然後按一下* 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、* ObjectGuid至Name 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*。
- 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. 按一下「完成」、然後按一下「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、或只是手動輸入值。

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 到「還原」和 ["測試所有依賴方信任"](#) 以確認設定正確。

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。

您需要的產品

- 您已將SSO設定為StorageGRID「支援」、而且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。

- 您有上傳的StorageGRID 自訂憑證供您使用、或者您知道如何從命令Shell登入管理節點。
- 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。

關於這項工作

這些指示適用於Windows Server 2016隨附的AD FS 4.0。如果您使用的是Windows 2012 R2隨附的AD FS 3.0、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。

步驟

1. 在Windows Server Manager中、按一下*「工具」、然後選取「AD FS管理*」。
2. 在「Actions（動作）」下、按一下「* Add S依賴方Trust（*新增
3. 在歡迎頁面上、選擇* Claims感知*、然後按一下*開始*。

4. 選取*手動輸入依賴方的相關資料*、然後按一下*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、請按一下*「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）、然後按一下* 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、* ObjectGuid至Name 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*。

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. 按一下「完成」、然後按一下「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. 單擊* 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. 按一下「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. 按一下「套用」、然後按一下「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 到「還原」和 "測試所有依賴方信任" 以確認設定正確。

測試依賴方信任

在您強制使用單一登入 (SSO) 來StorageGRID 執行動作之前、請先確認單一登入和單一登出 (SLO) 設定正確。如果您為每個管理節點建立了依賴方信任、請確認您可以針對每個管理節點使用SSO和SLO。

您需要的產品

- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須擁有特定的存取權限。
- 您已在AD FS中設定一或多個信賴關係人信任。

步驟

1. 選擇*組態*存取控制*單一登入*。

單一登入頁面隨即出現、並已選取* Sandbox Mode*選項。
2. 在沙箱模式的指示中、找到您身分識別供應商登入頁面的連結。

此URL衍生自您在*聯盟服務名稱*欄位中輸入的值。

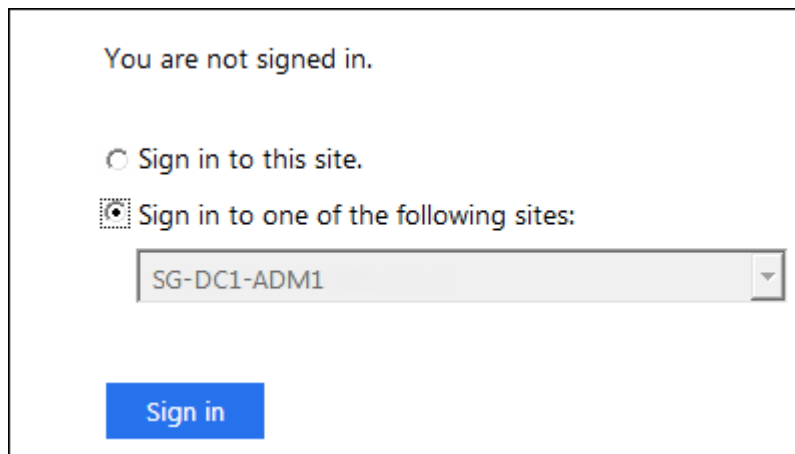
Sandbox mode

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.

3. 按一下連結、或複製URL並貼到瀏覽器、即可存取身分識別供應商的登入頁面。
4. 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*、選取主要管理節點的依賴方識別碼、然後按一下*登入*。



系統會提示您輸入使用者名稱和密碼。

5. 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。

✔ 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。

6. 重複上述步驟、確認您可以登入任何其他管理節點。

如果所有SSO登入和登出作業都成功、您就可以啟用SSO。

啟用單一登入

在使用沙箱模式測試StorageGRID 所有的不依賴方信任之後、您就可以開始啟用單一登入 (SSO)。

您需要的產品

- 您必須從身分識別來源匯入至少一個同盟群組、並將「根存取」管理權限指派給群組。您必須確認至少有一位同盟使用者擁有Grid Manager的「根存取」權限、以及任何現有租戶帳戶的「租戶管理程式」權限。
- 您必須使用沙箱模式測試所有依賴方信任。

步驟

1. 選擇*組態*存取控制*單一登入*。

單一登入頁面隨即顯示、並選取*沙箱模式*。

2. 將SSO狀態變更為*已啟用*。
3. 按一下「*儲存*」。

出現警告訊息。

Warning

Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. 檢閱警告、然後按一下「確定」。

現在已啟用單一登入。



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。

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。

您需要的產品

- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須擁有特定的存取權限。

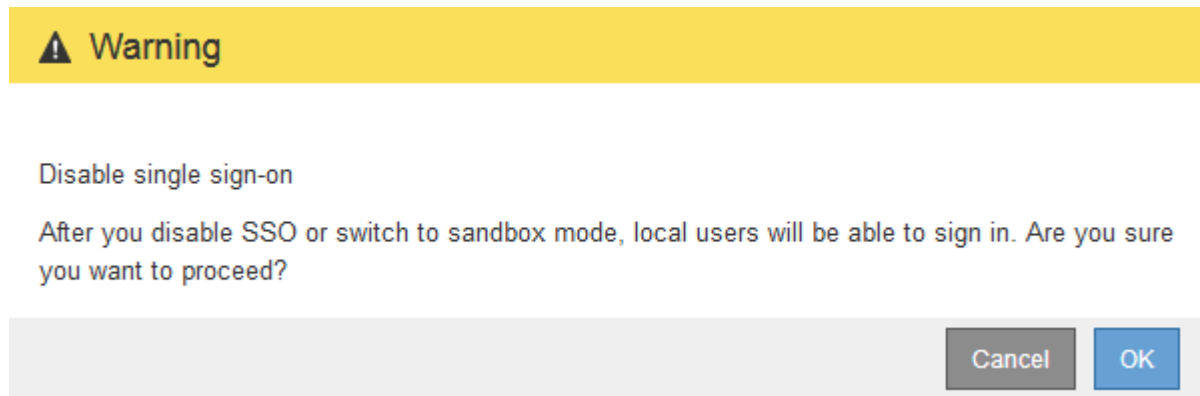
步驟

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. 按一下「*儲存*」。

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. 按一下「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。

暫時停用及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。

您需要的產品

- 您必須擁有特定的存取權限。
- 您必須擁有 Passwords.txt 檔案：
- 您必須知道本機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SSSSO*」核取方塊會保持選取狀態、除非您更新所有現有的SSO設定、否則這些設定都會維持不變。

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. 按一下「*儲存*」。

按一下「單一登入」頁面中的「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. 按一下*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。

相關資訊

["設定單一登入"](#)

版權資訊

Copyright © 2024 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。