



# 控制系統管理員存取**StorageGRID** 功能

## StorageGRID 11.5

NetApp  
April 11, 2024

# 目錄

控制系統管理員存取StorageGRID 功能 .....	1
透過防火牆控制存取 .....	1
使用身分識別聯盟 .....	2
管理管理群組 .....	7
管理本機使用者 .....	15
使用單一登入 (SSO) StorageGRID 進行支援 .....	17
設定系統管理員用戶端憑證 .....	35

# 控制系統管理員存取StorageGRID 功能

您可以開啟StorageGRID 或關閉防火牆連接埠、管理管理群組和使用者、設定單一登入 (SSO) 、以及提供用戶端憑證、以便安全地從外部存取StorageGRID 各項效能數據、藉此控制管理員對該系統的存取。

- "透過防火牆控制存取"
- "使用身分識別聯盟"
- "管理管理群組"
- "管理本機使用者"
- "使用單一登入 (SSO) StorageGRID 進行支援"
- "設定系統管理員用戶端憑證"

## 透過防火牆控制存取

當您想要透過防火牆控制存取時、可以在外部防火牆開啟或關閉特定的連接埠。

### 控制外部防火牆的存取

您可以StorageGRID 在外部防火牆開啟或關閉特定連接埠、以控制對使用者介面和API的存取。例如、除了使用其他方法來控制系統存取之外、您可能還想要防止租戶連線到防火牆的Grid Manager。

連接埠	說明	如果連接埠已開啟...
443..	管理節點的預設HTTPS連接埠	Web瀏覽器和API用戶端可存取Grid Manager、Grid Management API、租戶管理程式和租戶管理API。  *附註：*連接埠443也用於部分內部流量。
8443.	管理節點上的受限網格管理器連接埠	<ul style="list-style-type: none"><li>• Web瀏覽器和API用戶端可使用HTTPS存取Grid Manager和Grid Management API。</li><li>• Web瀏覽器和API用戶端無法存取租戶管理程式或租戶管理API。</li><li>• 系統將拒絕內部內容的要求。</li></ul>
9443	管理節點上的受限租戶管理程式連接埠	<ul style="list-style-type: none"><li>• Web瀏覽器和API用戶端可使用HTTPS存取租戶管理程式和租戶管理API。</li><li>• Web瀏覽器和API用戶端無法存取Grid Manager或Grid Management API。</li><li>• 系統將拒絕內部內容的要求。</li></ul>



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)。

#### 相關資訊

["登入Grid Manager"](#)

["如果StorageGRID 無法使用SSO、請建立租戶帳戶"](#)

["摘要：用於用戶端連線的IP位址和連接埠"](#)

["管理不受信任的用戶端網路"](#)

["安裝Ubuntu或DEBIAN"](#)

["安裝VMware"](#)

["安裝Red Hat Enterprise Linux或CentOS"](#)

## 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。

### 設定身分識別聯盟

如果您想要在另一個系統 (例如Active Directory、OpenLDAP或Oracle Directory Server) 中管理管理系統群組和使用者、可以設定身分識別聯盟。

#### 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。
- 如果您打算啟用單一登入 (SSO)、則必須使用Active Directory做為聯盟身分識別來源、使用AD FS做為身分識別供應商。請參閱「使用單一登入的要求」。
- 您必須使用Active Directory、OpenLDAP或Oracle Directory Server做為身分識別供應商。



如果您要使用未列出的LDAP v3服務、則必須聯絡技術支援部門。

- 如果您打算使用傳輸層安全性 (TLS) 與LDAP伺服器進行通訊、則身分識別供應商必須使用TLS 1.2或1.3。

#### 關於這項工作

若要匯入下列類型的聯盟群組、您必須為Grid Manager設定身分識別來源：

- 系統管理群組：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。
- 租戶使用者群組、適用於不使用自己身分識別來源的租戶。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。

#### 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\*。

此時會顯示用於設定LDAP伺服器的欄位。

3. 在LDAP服務類型區段中、選取您要設定的LDAP服務類型。

您可以選擇\* Active Directory 、 OpenLDAP\*或\*其他\*。



如果選擇\* OpenLDAP\*、則必須設定OpenLDAP伺服器。請參閱OpenLDAP伺服器設定指南。



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。

- 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. 在「Configure LDAP server (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伺服器的伺服器主機名稱或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`

- 密碼：與使用者名稱相關的密碼。
- 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。

6. 在\*傳輸層安全性（TLS）\*區段中、選取安全性設定。

- 使用**ARTTLS**（建議使用）：使用ARTTLS來保護與LDAP伺服器的通訊安全。這是建議的選項。
- 使用**LDAPS**：LDAPS（LDAP over SSL）選項使用TLS建立與LDAP伺服器的連線。基於相容性考量、支援此選項。
- 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。



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。

8. 或者、選取\*測試連線\*來驗證LDAP伺服器的連線設定。

如果連線有效、頁面右上角會出現確認訊息。

9. 如果連線有效、請選取\*儲存\*。

下列螢幕擷取畫面顯示使用Active Directory之LDAP伺服器的組態值範例。

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

## Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

••••••••

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

相關資訊

["用於傳出TLS連線的支援密碼"](#)

["使用單一登入的需求"](#)

["建立租戶帳戶"](#)

["使用租戶帳戶"](#)

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。

## memberOf和refert覆疊

應啟用memberOf和refert覆疊。如需詳細資訊、請參閱OpenLDAP管理員指南中的反轉群組成員資格維護說明。

### 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OpenLDAP系統管理員指南中有關反轉群組成員資格維護的資訊。

### 相關資訊

["OpenLDAP文件：2.4版管理員指南"](#)

## 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。

### 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。
- 必須啟用身分識別來源。

### 步驟

1. 選擇\*組態\*>\*存取控制\*>\*身分識別聯盟\*。

此時會出現「身分識別聯盟」頁面。「同步處理」按鈕位於頁面底部。

#### Synchronize

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

2. 單擊\* Synchronize\*。

確認訊息表示同步已成功啟動。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。

### 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

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。
- 如果單一登入 (SSO) 設定為\*已啟用\*或\*沙箱模式\*、則「啟用身分聯盟」核取方塊會停用。「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。

### 步驟

1. 選擇\*組態\*>\*存取控制\*>\*身分識別聯盟\*。
2. 取消核取「啟用身分識別聯盟」核取方塊。
3. 按一下「\*儲存\*」。

### 相關資訊

["停用單一登入"](#)

## 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。

### 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。

### 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。
- 如果您打算匯入聯盟群組、則必須已設定身分識別聯盟、而且聯盟群組必須已存在於已設定的身分識別來源中。

### 步驟

1. 選擇\*組態\*存取控制\*管理群組\*。

此時將顯示「管理群組」頁面、並列出任何現有的管理群組。

## Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.

<input type="button" value="+ Add"/> <input type="button" value="Clone"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>				
	Name	ID	Group Type	Access Mode
<input checked="" type="radio"/>	Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/>	Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
<input type="radio"/>	ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/>	API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/>	ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/>	Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write


Group Type  Show  rows per page

2. 選取\*「Add\*」。

此時會出現「新增群組」對話方塊。


## Add Group

Create a new local group or import a group from the external identity source.












Group Type   Local  Federated

Display Name

Unique Name 

Access Mode   Read-write  Read-only

### Management Permissions

- |  |   |
|--|---|
| <input type="checkbox"/> Root Access                  | <input type="checkbox"/> Manage Alerts                     |
| <input type="checkbox"/> Acknowledge Alarms           | <input type="checkbox"/> Grid Topology Page Configuration  |
| <input type="checkbox"/> Other Grid Configuration     | <input type="checkbox"/> Tenant Accounts                   |
| <input type="checkbox"/> Change Tenant Root Password  | <input type="checkbox"/> Maintenance                       |
| <input type="checkbox"/> Metrics Query                | <input type="checkbox"/> ILM                                 |
| <input type="checkbox"/> Object Metadata Lookup      | <input type="checkbox"/> Storage Appliance Administrator  |

Cancel

Save

- 對於群組類型、如果您想要建立僅在StorageGRID 內部使用的群組、請選取\*本機\*；如果您想從身分識別來源匯入群組、請選取\*聯盟\*。
- 如果您選取\*本機\*、請輸入群組的顯示名稱。顯示名稱是顯示在Grid Manager中的名稱。例如「維護使用者」或「ILM管理員」。
- 輸入群組的唯一名稱。
  - 本機：輸入您想要的任何唯一名稱。例如、「ILM管理員」。
  - 聯盟：輸入與設定的身分識別來源中所顯示的群組名稱完全相同的名稱。
- 對於\*存取模式\*、選取群組中的使用者是否可以變更網格管理程式和網格管理API中的設定及執行作業、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。

- 選取一或多個管理權限。

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。

## 8. 選擇\*保存\*。

隨即建立新群組。如果這是本機群組、您現在可以新增一或多個使用者。如果這是聯盟群組、身分識別來源會管理屬於該群組的使用者。

相關資訊

["管理本機使用者"](#)

## 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。

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）
- 在「組態與維護」頁面上檢視特定資訊

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。

### 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。

### 認可警報（舊系統）

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。

### 網格拓撲頁面組態

此權限可讓您存取下列功能表選項：

- 組態索引標籤可從\*支援\*工具\* Grid拓撲\*的頁面取得。
- 「\*節點\*事件」索引標籤上的「重設事件數\*」連結。

## 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。

- 警報（舊系統）：
  - 全域警示
  - 舊版電子郵件設定
- \* ILM \*：
  - 儲存資源池
  - 儲存等級
- 組態\*網路設定
  - 連結成本
- 組態\*系統設定：
  - 顯示選項
  - 網格選項
  - 儲存選項
- 組態\*監控：
  - 活動
- 支援：
  - AutoSupport

## 租戶帳戶

此權限可讓您存取「租戶\*租戶帳戶」頁面。



Grid Management API第1版（已過時）使用此權限來管理租戶群組原則、重設Swift管理密碼、以及管理root使用者S3存取金鑰。

## 變更租戶根密碼

此權限可讓您存取「租戶帳戶」頁面上的\*變更根密碼\*選項、讓您控制誰可以變更租戶本機根使用者的密碼。沒有此權限的使用者將無法看到\*變更根密碼\*選項。



您必須先將「租戶帳戶」權限指派給群組、才能指派此權限。

## 維護

此權限可讓您存取下列功能表選項：

- 組態\*系統設定：
  - 網域名稱\*
  - 伺服器憑證\*
- 組態\*監控：
  - 稽核\*
- 組態\*存取控制：
  - 網格密碼
- 維護\*維護工作\*
  - 取消委任
  - 擴充
  - 恢復
- 維護\*網路\*：
  - DNS伺服器\*
  - 網格網路\*
  - NTP伺服器\*
- 維護\*系統\*：
  - 授權\*
  - 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、但不能編輯標有星號的頁面。

## 度量查詢

此權限可讓您存取\*支援\*工具\*指標\*頁面。此權限也可讓您使用**Grid Management API**的 Metrics \*區段、存取自訂的Prometheus度量查詢。

## ILM

此權限可讓您存取下列\* ILM \*功能表選項：

- 刪除編碼
- 規則
- 政策
- 地區



存取\* ILM \* **Storage Pools**\*和 ILM \* Storage Elgres\*功能表選項是由其他Grid Configuration 和Grid拓撲頁面組態權限所控制。

### 物件中繼資料查詢

此權限可讓您存取\* ILM \*物件中繼資料查閱\*功能表選項。

### 儲存設備管理員

此權限可SANtricity 讓您透過Grid Manager存取儲存設備上的E系列支援系統管理程式。

### 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、或是否只能檢視相關的設定和功能。如果使用者屬於多個群組、且任何群組設定為\*唯讀\*、則使用者將擁有所有選取設定和功能的唯讀存取權。

### 從Grid Management API停用功能

您可以使用Grid Management API來完全停用StorageGRID 作業系統中的某些功能。停用某項功能時、將無法指派權限給任何人、以執行與該功能相關的工作。

#### 關於這項工作

停用的功能系統可讓您防止存取StorageGRID 某些功能。停用功能是防止擁有「根存取」權限的root使用者或屬於管理群組的使用者能夠使用該功能的唯一方法。

若要瞭解此功能的用途、請考慮下列案例：

公司A是一家服務供應商、*StorageGRID* 負責建立租戶帳戶、以租賃其所屬的一套系統的儲存容量。為了保護租戶物件的安全、A公司希望確保其員工在部署帳戶後、永遠無法存取任何租戶帳戶。

公司A可以使用Grid Management API中的Deactivate Features系統來達成此目標。透過完全停用Grid Manager (UI和API) 中的\*變更租戶根密碼\*功能、公司A可確保任何管理員使用者（包括root使用者和擁有root存取權限的群組使用者）都無法變更任何租戶帳戶根使用者的密碼

#### 重新啟動停用的功能

根據預設、您可以使用Grid Management API重新啟動已停用的功能。不過、如果您想要防止停用的功能再次被重新啟動、您可以停用\*啟用功能\*功能本身。



無法重新啟動\*活動功能\*功能。如果您決定停用此功能、請注意、您將永遠喪失重新啟動任何其他停用功能的能力。您必須聯絡技術支援部門、才能恢復任何喪失的功能。

如需詳細資訊、請參閱實作S3或Swift用戶端應用程式的指示。

#### 步驟

1. 存取Grid Management API的Swagger文件。
2. 找出停用功能端點。
3. 若要停用功能、例如\*變更租戶根密碼\*、請將本文傳送至API、如下所示：

```
{ "grid": {"changeTenantRootPassword": true} }
```

申請完成後、「變更租戶根密碼」功能會停用。變更租戶根密碼管理權限不再出現在使用者介面中、任何嘗試變更租戶根密碼的API要求都會失敗、並顯示「403 Forbidden」。

- 若要重新啟動所有功能、請將本文傳送至API、如下所示：

```
{ "grid": null }
```

完成此要求後、所有功能（包括變更租戶根密碼功能）都會重新啟動。變更租戶根密碼管理權限現在會出現使用者介面中、而且任何嘗試變更租戶根密碼的API要求都會成功、前提是使用者具有根存取權限或變更租戶根密碼管理權限。



上一個範例會重新啟動\_all\_停用的功能。如果停用其他應保持停用狀態的功能、您必須在PUT要求中明確指定這些功能。例如、若要重新啟動「變更租戶根密碼」功能並繼續停用「警報確認」功能、請傳送此「PUT」要求：

```
{ "grid": { "alarmAcknowledgment": true } }
```

## 相關資訊

### ["使用Grid Management API"](#)

## 修改管理群組

您可以修改管理群組、以變更與群組相關的權限。對於本機管理群組、您也可以更新顯示名稱。

### 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\*管理群組\*。
2. 選取群組。

如果您的系統包含20個以上的項目、您可以指定一次在每個頁面上顯示的列數。然後、您可以使用瀏覽器的「尋找」功能、在目前顯示的列中搜尋特定項目。

3. 按一下 \* 編輯 \*。
4. 或者、對於本機群組、請輸入使用者會看到的群組名稱、例如「維護使用者」。

您無法變更唯一名稱、也就是內部群組名稱。

5. 您也可以變更群組的存取模式。



- 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。

6. 您也可以選擇新增或移除群組權限。

請參閱管理群組權限的相關資訊。

7. 選擇\*保存\*。

相關資訊

[\[管理群組權限\]](#)

## 刪除管理群組

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管理使用者、但不會刪除管理使用者。

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

刪除群組時、指派給該群組的使用者將喪失Grid Manager的所有存取權限、除非他們被其他群組授予權限。

步驟

1. 選擇\*組態\*存取控制\*管理群組\*。
2. 選取群組名稱。

如果您的系統包含20個以上的項目、您可以指定一次在每個頁面上顯示的列數。然後、您可以使用瀏覽器的「尋找」功能、在目前顯示的列中搜尋特定項目。

3. 選擇\*移除\*。
4. 選擇\*確定\*。

## 管理本機使用者

您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。

Grid Manager包含一個預先定義的本機使用者、名為「root」。雖然您可以新增及移除本機使用者、但無法移除root使用者。



如果已啟用單一登入（SSO）、則本機使用者無法登入StorageGRID 到畫面。

- 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。

## 建立本機使用者

如果您已建立本機管理群組、則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群組。群組的權限可控制使用者可以存取的Grid Manager功能。

### 關於這項工作

您只能建立本機使用者、而且只能將這些使用者指派給本機管理群組。同盟使用者和同盟群組是使用外部身分識別來源進行管理。

### 步驟

1. 選擇\*組態\*>\*存取控制\*>\*管理使用者\*。
2. 按一下「\* 建立 \*」。
3. 輸入使用者的顯示名稱、唯一名稱和密碼。
4. 將使用者指派給一或多個控制存取權限的群組。

群組名稱清單是從群組表格產生的。

5. 按一下「\* 儲存 \*」。

### 相關資訊

["管理管理群組"](#)

## 修改本機使用者的帳戶

您可以修改本機管理員使用者的帳戶、以更新使用者的顯示名稱或群組成員資格。您也可以暫時禁止使用者存取系統。

### 關於這項工作

您只能編輯本機使用者。同盟使用者詳細資料會自動與外部身分識別來源同步。

### 步驟

1. 選擇\*組態\*>\*存取控制\*>\*管理使用者\*。
2. 選取您要編輯的使用者。

如果您的系統包含20個以上的項目、您可以指定一次在每個頁面上顯示的列數。然後、您可以使用瀏覽器的「尋找」功能、在目前顯示的列中搜尋特定項目。

3. 按一下 \* 編輯 \*。
4. 您也可以選擇變更名稱或群組成員資格。
5. 或者、若要防止使用者暫時存取系統、請勾選\*拒絕存取\*。

6. 按一下「\* 儲存 \*」。

新設定會在使用者下次登出後重新登入Grid Manager時套用。

## 刪除本機使用者的帳戶

您可以刪除不再需要存取Grid Manager的本機使用者帳戶。

### 步驟

1. 選擇\*組態\*>\*存取控制\*>\*管理使用者\*。
2. 選取您要刪除的本機使用者。



您無法刪除預先定義的根本機使用者。

如果您的系統包含20個以上的項目、您可以指定一次在每個頁面上顯示的列數。然後、您可以使用瀏覽器的「尋找」功能、在目前顯示的列中搜尋特定項目。

3. 按一下「移除」。
4. 按一下「確定」。

## 變更本機使用者的密碼

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。此外、具有「管理使用者」頁面存取權的使用者、也可以變更其他本機使用者的密碼。

### 關於這項工作

您只能變更本機使用者的密碼。同盟使用者必須在外部身分識別來源中變更自己的密碼。

### 步驟

1. 選擇\*組態\*>\*存取控制\*>\*管理使用者\*。
2. 從「使用者」頁面選取使用者。

如果您的系統包含20個以上的項目、您可以指定一次在每個頁面上顯示的列數。然後、您可以使用瀏覽器的「尋找」功能、在目前顯示的列中搜尋特定項目。

3. 按一下\*變更密碼\*。
4. 輸入並確認密碼、然後按一下\*「Save\*（儲存\*）」。

## 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

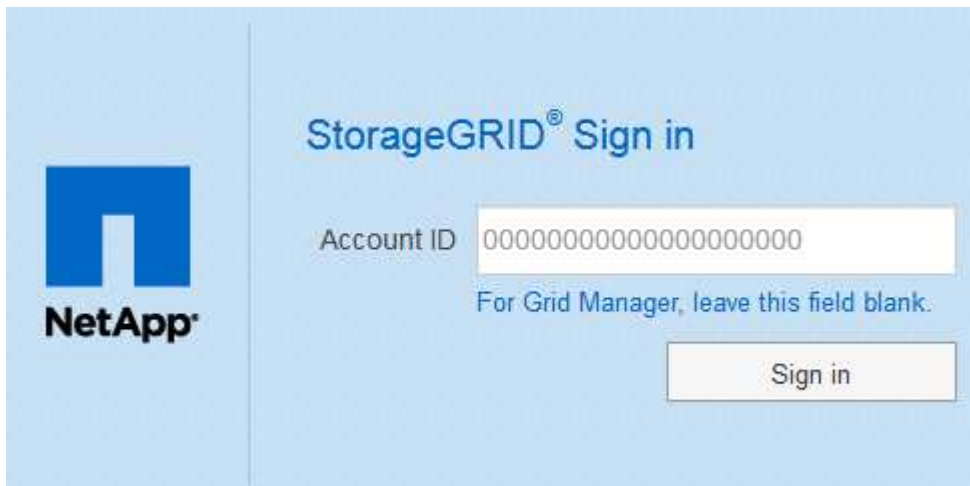
啟用SSO並登入StorageGRID 支援功能時、系統會將您重新導向至組織的SSO頁面、以驗證您的認證資料。

#### 步驟

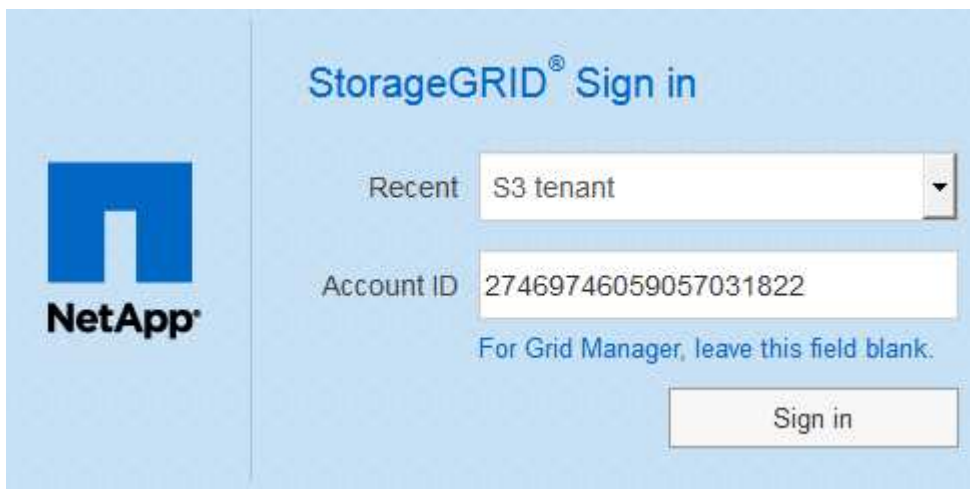
1. 在StorageGRID 網頁瀏覽器中輸入任何「靜態管理節點」的完整網域名稱或IP位址。

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：



- 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. 按一下\*登入\*

可將您重新導向至組織的SSO登入頁面。StorageGRID例如：

Sign in with your organizational account

someone@example.com

Password

Sign in

4. `[[signin_SSO ]`使用您的SSO認證登入。

如果SSO認證資料正確：

- 身分識別供應商（IDP）提供驗證回應StorageGRID 功能以回應功能。
- 驗證驗證回應。StorageGRID
- 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)  GB ▼

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) 能夠安全地使用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：

- a. 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。

- b. 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。

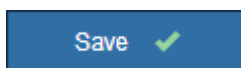
- 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

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。



- 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_Identifier" -MetadataURL  
"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. 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。



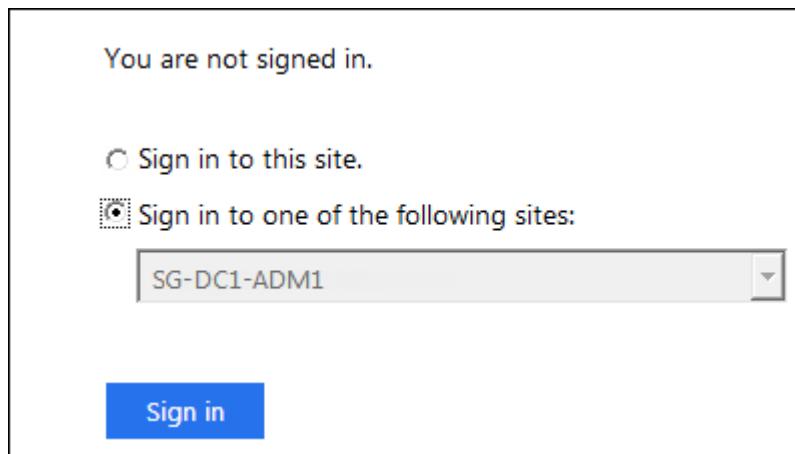
## Sandbox mode

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。

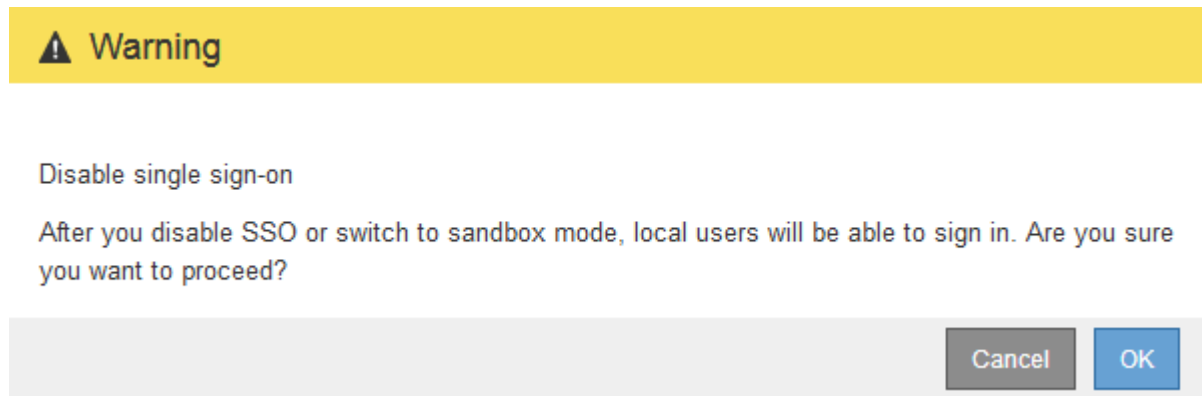
#### 步驟

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SSO\*」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"](#)

## 設定系統管理員用戶端憑證

您可以使用用戶端憑證、讓授權的外部用戶端存取StorageGRID 《The》介紹的資料庫。用戶端憑證提供安全的方法、讓您使用外部工具來監控StorageGRID VMware。

如果您需要StorageGRID 使用外部監控工具存取功能、則必須使用Grid Manager上傳或產生用戶端憑證、並將憑證資訊複製到外部工具。

### 新增系統管理員用戶端憑證

若要新增用戶端憑證、您可以提供自己的憑證、或使用Grid Manager產生一個憑證。

您需要的產品

- 您必須具有「根存取」權限。
- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須知道管理節點的IP位址或網域名稱。
- 您必須已設定StorageGRID 「無法使用的介面伺服器憑證」、並擁有對應的CA套裝組合
- 如果您要上傳自己的憑證、則憑證的公開金鑰和私密金鑰必須在本機電腦上可用。

步驟

1. 在Grid Manager中、選取\*組態\*>\*存取控制\*>\*用戶端憑證\*。

此時會出現「用戶端憑證」頁面。

#### Client Certificates


You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.




2. 選取\*「Add\*」。

隨即顯示「上傳憑證」頁面。

Upload Certificate

Name 

Allow Prometheus 

**Certificate Details**


Upload the public key for the client certificate.

3. 輸入一個介於1到32個字元之間的憑證名稱。
4. 若要使用外部監控工具存取Prometheus指標、請選取\*允許Prometheus\*核取方塊。
5. 上傳或產生憑證：
  - a. 若要上傳憑證、請前往 [請按這裡](#)。
  - b. 若要產生憑證、請執行 [請按這裡](#)。
6. `[[upload_cert ]`若要上傳憑證：
  - a. 選擇\*上傳用戶端憑證\*。
  - b. 瀏覽憑證的公開金鑰。

上傳憑證的公開金鑰之後、會填入\*憑證中繼資料\*和\*憑證PEP\*欄位。

## Upload Certificate

Name  test-certificate-upload

Allow Prometheus 


### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata 

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoOgAwIBAgIUDDQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwdDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbgG1mb3JuaWEwEjAQBgNVBAcM
CVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1N1oXDTEwMDYx
OTIyMTE1N1owDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbgG1mb3JuaWEwEjAQB
BgNVBAcMCVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xCzAJBgNVBAsM
Ak1UMRkwFwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAsVqq2MnjvVotLeStq1Co4coJmsQ2ygRhuwSza0bgMnjf
cWUgHNVPXGuGlzY/Tl37r3Dk5bu2fyGYAeJ6mqbQA6cE3yp0p5Hw7Cm/AWJknFw6
```

Copy certificate to clipboard

Cancel


Save

- a. 選取\*將憑證複製到剪貼簿\*、然後將憑證貼到外部監控工具。
  - b. 使用編輯工具將私密金鑰複製並貼到外部監控工具。
  - c. 選取\*「儲存\*」、將憑證儲存在Grid Manager中。
7. [generate\_cert ]若要產生憑證：
- a. 選擇\*產生用戶端憑證\*。
  - b. 輸入管理節點的網域名稱或IP位址。
  - c. 您也可以輸入一個X.509主題（也稱為辨別名稱（DN））、以識別擁有該憑證的系統管理員。
  - d. 或者、選取憑證有效的天數。預設值為730天。
  - e. 選取\*產生\*。

「憑證中繼資料」、「憑證PEP」及「憑證私密金鑰」欄位會填入。

## Upload Certificate

Name  test-certificate-generate

Allow Prometheus 

### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Certificate metadata 

```
Subject DN: /CN=test.com
Serial Number: 08:F8:FB:76:B2:13:E4:DF:54:83:3D:35:56:0F:2A:03:53:B0:E2:0
A
Issuer DN: /CN=test.com
Issued On: 2020-11-20T22:44:46.000Z
Expires On: 2022-11-20T22:44:46.000Z
SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:88:E4:C6:42:52:5F:32:7E:E7:93:66:89:F3:3
D
SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:
EF:78:C0:A4:66:C2:EB:65:64:C3:D4:7A:B0
```

Certificate PEM 


```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUUCFj7dxITSN9Ugs01Vm8qA1Ow4gowDQYJKoZIhvcNAQEL
BQAwEwERMA8GA1UEAwwIdGVzZC5jb20wHhcNMjIwMjI0MjI0NDQ2WWhcNMjIwMjI0
MjI0NDQ2WjATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASAwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAR02dS9mx2jFrGuBb22Mjcidf/tTcKxLtB9m+4vIwt1gvrR
XgHZ31B9YIqn/Vo729R2mNKKyBwkyQTkGCO2Ixvv0STBLEIWFb8sTgcIcMyt1V1F
OseBWy402xxjnR3/X+AX+6s2WZIsVe+3CDjGu4ie0V/uVQxx4yA1T9SoKnjBmOa
LCVjL6iVnkUGB8GbkYUPeOaoMjsL6TN1QsoFv9VEB0xBKCP4D7FDbaIy2f9Ng8rS
FEOQoLNtN=XCasLO4D7j2qFqOVUpFJ3M0oh1x0n5pQ78Z5KfYwVvDKg6v52P8UBM
1o6GeuoFaW+dbpLZKp09N1VtFhghXe9AxxN8s+kCAwEAAaMXMBUwEwYDVR0RBBAww
-----
```

Copy certificate to clipboard

Certificate private key 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEARtZ0H2bHaM+sa4Fv2kyNyJ1/+1NwzEu0Eab7i8jC2KNC/BFe
AdneUH1ghCf9Wjvb1HaY0oxIHCTJBOQYI5kjG+/RjMEb4h29sKxOBwizgK2VWUU7
OwFZjPg7bFGOorf9f4Bf7xN1ZkixV75IICMa7iJaRX+5VDPHjIDVP1KggelMGYSos
JWmVqJwRQYFI2uTJQ946qgyOwvpm2VDOgW/1UQHTEEoKngFpUNtojLZ/02DmtJ8
Q8Cg=202x0JxMe7gFuNmoWe5hS8Uncw6iHXHSfmlDvxnkp9jBw0MqDm/nY/xQEw
jw266h9pbS1ukt2k703VW0WGCfD7GDPE2yyQIDAQAABoIBAQCfEUfY4pE0Hqtv
2uEL6De4yXMTwg/Sgn+W3mvtgdgQB4xWEGQrk1kEUG+HTYrFJen6XX0vACDYAC/
Hh1Q67xDPVpRjdpuK0tr1W3ervsEmpBx99MqH9Y2UGw6Yub3UBJaqfDvja4Nvaon
MxaYJRFBLvAR7f2z2xXV5b0zRPA+rn0YCrz1Lct5Y0K79e0G8naTmwIdm2YM6EE
-----
```

Copy private key to clipboard

 You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

Cancel

Save

- a. 選取\*將憑證複製到剪貼簿\*、然後將憑證貼到外部監控工具。
- b. 選取\*將私密金鑰複製到剪貼簿\*、然後將金鑰貼到外部監控工具。



關閉對話方塊後、您將無法檢視私密金鑰。將金鑰複製到安全位置。

- c. 選取\*「儲存\*」、將憑證儲存在Grid Manager中。
8. 在外部監控工具（例如Grafana）上設定下列設定。



Grafana範例顯示於下列螢幕快照中：

Name ⓘ  Default

### HTTP

URL ⓘ

Access  ▼ [Help >](#)

Whitelisted Cookies ⓘ  [Add](#)

### Auth

Basic auth  With Credentials ⓘ

TLS Client Auth  With CA Cert ⓘ

Skip TLS Verify

Forward OAuth Identity ⓘ

### TLS/SSL Auth Details ⓘ

CA Cert

ServerName

Client Cert

a. 名稱：輸入連線名稱。

不需要此資訊、但您必須提供名稱來測試連線。StorageGRID

b. \* URL\*：輸入管理節點的網域名稱或IP位址。指定HTTPS和連接埠9091。

例如：`https://admin-node.example.com:9091`

- c. 啟用\* TLS用戶端授權\*和\* CA認證\*。
- d. 將管理介面伺服器憑證或CA套件複製並貼到「TLS/SSL驗證詳細資料」下的「\*\*CA認證」。
- e. 伺服器名稱：輸入管理節點的網域名稱。

伺服器名稱必須符合管理介面伺服器憑證中顯示的網域名稱。

- f. 儲存並測試您從StorageGRID 餐廳或本機檔案複製的憑證和私密金鑰。

您現在可以StorageGRID 使用外部監控工具、從功能表上存取Prometheus指標。

如需指標的相關資訊、請參閱監控和疑難排解StorageGRID 的指示。

## 相關資訊

["使用StorageGRID 資訊安全認證"](#)

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

["監控安培；疑難排解"](#)

## 編輯系統管理員用戶端憑證

您可以編輯憑證以變更其名稱、啟用或停用Prometheus存取、或是在目前的憑證過期時上傳新的憑證。

### 您需要的產品

- 您必須具有「根存取」權限。
- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須知道管理節點的IP位址或網域名稱。
- 如果您要上傳新的憑證和私密金鑰、則必須可在本機電腦上使用這些憑證和私密金鑰。

### 步驟

1. 選擇\*組態\*>\*存取控制\*>\*用戶端憑證\*。

此時會出現「用戶端憑證」頁面。列出現有的憑證。

下表列出憑證到期日。如果憑證即將到期或已過期、表格中會出現訊息、並觸發警示。

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. 選取您要編輯之憑證左側的選項按鈕。
3. 選擇\*編輯\*。

「編輯憑證」對話方塊隨即出現。

### Edit Certificate test-certificate-generate

Name

Allow Prometheus

#### Certificate Details

Upload the public key for the client certificate.

Certificate metadata

```
Subject DN: /CN=test.com
Serial Number: 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53
Issuer DN: /CN=test.com
Issued On: 2020-11-23T15:53:33.000Z
Expires On: 2022-11-23T15:53:33.000Z
SHA-1 Fingerprint: AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7
SHA-256 Fingerprint: 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:9
0:EC:7A:7B:EF:23:14:55:3D:56
```

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAwezERMAsGA1UEAwIdGVzdC5jb20wHhcNMjAxMTIzMTU1MzZlMzUzNjIz
MTU1MzZlMzUzNjIzATMREwEwYDQDDAh0ZXN0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAKdgceneCDFDsLjvLnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkW05a2Mym7EhbNrfwOt2nMjQkcaKIrk8OAmutRgG6N1N12FIW0qY0uzFQ0QddLq
n7ymFk6wSa9zYSu7Lp84Yn0/LSDPk+h3Jio7Mrt2X70It5ZDRwFmbLNvEvYEtTS
h+FbNh885AIRO2eLxvC0IRij1by8e7EwK+Wmc97HdxRSgyxIWk6BD47XC+d0rv55
wvtjc/41qc5xsE6XmJs2yJg4VARr10y8Icwa9fz00+xPwIdC0NwXkpWJXeBnCoXx
YqQxbWzjz+iVLJqLTMxU8zTTT30zUgN00M82GJUCAwEAAaMKMBUwEwYDVR0RBAAw
```

- 對憑證進行所需的變更。
- 選取\*「儲存\*」、將憑證儲存在Grid Manager中。
- 如果您上傳新的憑證：
  - 選取\*將憑證複製到剪貼簿\*、將憑證貼到外部監控工具。
  - 使用編輯工具將新的私密金鑰複製並貼到外部監控工具。
  - 在外部監控工具中儲存並測試憑證和私密金鑰。
- 如果您產生新的憑證：
  - 選取\*將憑證複製到剪貼簿\*、將憑證貼到外部監控工具。
  - 選取\*將私密金鑰複製到剪貼簿\*、將憑證貼到外部監控工具。



關閉對話方塊後、您將無法檢視或複製私密金鑰。將金鑰複製到安全位置。

- 在外部監控工具中儲存並測試憑證和私密金鑰。

## 移除系統管理員用戶端憑證

如果您不再需要憑證、可以將其移除。

您需要的產品

- 您必須具有「根存取」權限。
- 您必須使用支援的瀏覽器登入Grid Manager。

步驟

1. 選擇\*組態\*>\*存取控制\*>\*用戶端憑證\*。

此時會出現「用戶端憑證」頁面。列出現有的憑證。

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. 選取您要移除之憑證左側的選項按鈕。
3. 選擇\*移除\*。

隨即顯示確認對話方塊。

**Warning**

Delete certificate

Are you sure you want to delete the certificate "test-certificate-generate"?

Cancel OK

4. 選擇\*確定\*。

憑證即會移除。

## 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。