管理StorageGRID 一套系統

StorageGRID 11.5

NetApp
April 11, 2024

目錄

管理StorageGRID 一套系統

請使用這些指示來設定及管理StorageGRID 一套功能完善的系統。

這些說明說明說明如何使用Grid Manager來設定群組和使用者、建立租戶帳戶、讓S3和Swift用戶端應用程式儲存和擷取物件、設定和管理StorageGRID 各種不同的靜態網路、設定AutoSupport 各種功能、管理節點設定等。

使用資訊生命週期管理（ILM）規則和原則來管理物件的指示已移至"使用ILM管理物件"。

這些指示適用於StorageGRID 安裝好後、將會設定、管理及支援某個系統的技術人員。

您需要的產品

- 您大致瞭StorageGRID 解整個系統。
- 您對Linux命令Shell、網路及伺服器硬體設定與組態擁有相當詳細的知識。

網頁瀏覽器需求

您必須使用支援的網頁瀏覽器。

網頁瀏覽器	支援的最低版本
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84.

您應該將瀏覽器視窗設定為建議的寬度。

瀏覽器寬度	像素
最低	1024.
最佳化	1280

登入Grid Manager

您可以在支援的網頁瀏覽器的位址列中輸入管理節點的完整網域名稱（FQDN）或IP位址、以存取Grid Manager登入頁面。

您需要的產品

- 您必須擁有登入認證資料。
- 您必須擁有Grid Manager的URL。

- 您必須使用支援的網頁瀏覽器。
- Cookie必須在您的網路瀏覽器中啟用。
- 您必須擁有特定的存取權限。

關於這項工作

每StorageGRID 個系統包含一個主要管理節點和任意數量的非主要管理節點。您可以登入任何管理節點上的Grid Manager來管理StorageGRID 此系統。不過、管理節點並不完全相同：

- 在一個管理節點上發出的警示認可（舊系統）不會複製到其他管理節點。因此、針對警示所顯示的資訊在每個管理節點上可能看起來不一樣。
- 部分維護程序只能從主要管理節點執行。

如果管理節點包含在高可用度（HA）群組中、您可以使用HA群組的虛擬IP位址或對應至虛擬IP位址的完整網域名稱來連線。主要管理節點應選取為群組的慣用主節點、以便在存取Grid Manager時、在主要管理節點上存取、除非主要管理節點無法使用。

步驟

1. 啟動支援的網頁瀏覽器。
2. 在瀏覽器的網址列中、輸入Grid Manager的URL：

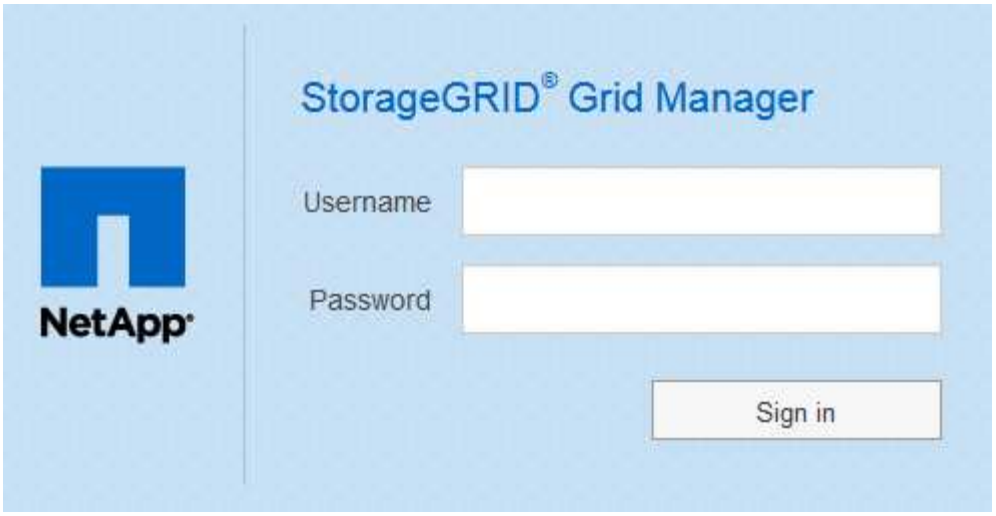
   `https://FQDN_or_Admin_Node_IP/`

   其中 *FQDN_or_Admin_Node_IP* 是管理節點的完整網域名稱或IP位址、或是管理節點的HA群組的虛擬IP位址。

   如果您必須在HTTPS（443）的標準連接埠以外的連接埠上存取Grid Manager、請輸入下列內容（其中）*FQDN_or_Admin_Node_IP* 是完整網域名稱或IP位址、連接埠是連接埠號碼：

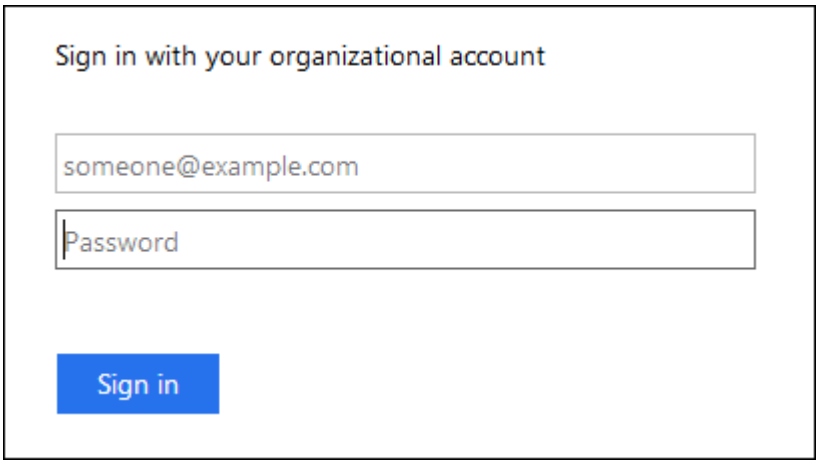
   `https://FQDN_or_Admin_Node_IP:port/`

3. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證。
4. 登入Grid Manager：
   - 如果StorageGRID 您的作業系統未使用單一登入（SSO）：
     i. 輸入Grid Manager的使用者名稱和密碼。
     ii. 按一下*登入*。



- 如果StorageGRID 您的系統啟用SSO、而且這是您第一次存取此瀏覽器上的URL：
  i. 按一下*登入*。您可以將「帳戶ID」欄位保留空白。

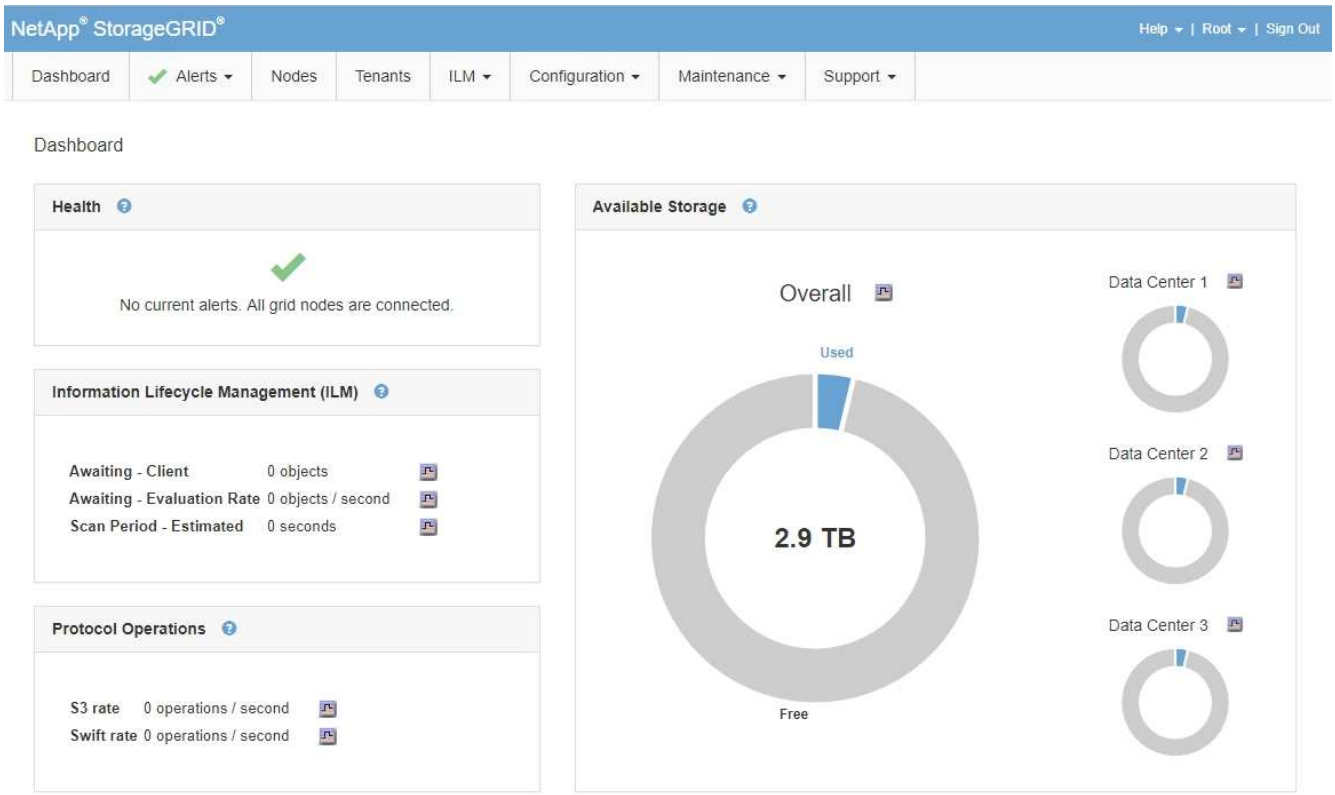
  ii. 在組織的SSO登入頁面上輸入標準SSO認證。例如：



- 如果StorageGRID 您的不支援系統已啟用SSO、且您先前曾存取Grid Manager或租戶帳戶：
  i. 執行下列任一項：

- 輸入* 0*（Grid Manager的帳戶ID）、然後按一下*登入*。
- 如果「* Grid Manager*」出現在最近的帳戶清單中、請選取該選項、然後按一下「登入」。

ii. 在組織的SSO登入頁面上、以標準SSO認證登入。當您登入時、會顯示Grid Manager的首頁、其中包括儀表板。如需瞭解提供的資訊、請參閱監控和疑難排解StorageGRID 說明中的「檢視儀表板」。



5. 若要登入其他管理節點：

選項	步驟
未啟用SSO	a. 在瀏覽器的位址列中、輸入其他管理節點的完整網域名稱或IP位址。視需要附上連接埠號碼。 b. 輸入Grid Manager的使用者名稱和密碼。 c. 按一下*登入*。
SSO已啟用	在瀏覽器的位址列中、輸入其他管理節點的完整網域名稱或IP位址。 如果您已登入一個管理節點、則無需再次登入、即可存取其他管理節點。不過、如果SSO工作階段過期、系統會再次提示您輸入認證資料。 附註： SSO無法在受限網格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

"網頁瀏覽器需求"

"透過防火牆控制存取"

"設定伺服器憑證"

"設定單一登入"

"管理管理群組"

"管理高可用度群組"

"使用租戶帳戶"

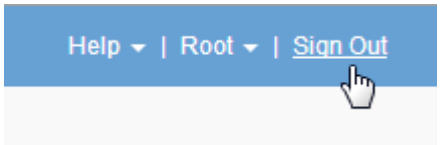
"監控安培；疑難排解"

登出Grid Manager

使用Grid Manager之後、您必須登出、以確保未獲授權的使用者無法存取StorageGRID 該系統。根據瀏覽器Cookie設定、關閉瀏覽器可能不會將您登出系統。

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*。

選項	說明
SSO未在使用中	您已登出管理節點。 此時會顯示Grid Manager登入頁面。 *附註：*如果您登入一個以上的管理節點、則必須登出每個節點。
SSO已啟用	您已登出您正在存取的所有管理節點。畫面上會顯示「這個登入頁面」StorageGRID 。網格管理器*在「*最近的帳戶」下拉式清單中列為預設值、*帳戶ID*欄位則顯示0。 *附註：*如果啟用SSO、而且您也已登入租戶管理程式、您也必須登出租戶帳戶、才能登出SSO。

相關資訊

"設定單一登入"

"使用租戶帳戶"

變更您的密碼

如果您是Grid Manager的本機使用者、可以變更自己的密碼。

您需要的產品

您必須使用支援的瀏覽器登入Grid Manager。

關於這項工作

如果StorageGRID 您以聯盟使用者的身分登入至支援單一登入（SSO）、則無法在Grid Manager中變更密碼。而是必須變更外部身分識別來源的密碼、例如Active Directory或OpenLDAP。

步驟

1. 從Grid Manager標頭中、選取*您的姓名_>變更密碼*。
2. 輸入您目前的密碼。
3. 輸入新密碼。

   您的密碼必須包含至少8個字元、且不得超過32個字元。密碼區分大小寫。

4. 重新輸入新密碼。
5. 按一下「 * 儲存 * 」。

變更資源配置通關密碼

請使用此程序來變更StorageGRID 供應密碼。恢復、擴充和維護程序需要通關密碼。下載恢復套件備份時、也需要密碼、其中包含適用於StorageGRID 整個系統的網格拓撲資訊和加密金鑰。

您需要的產品

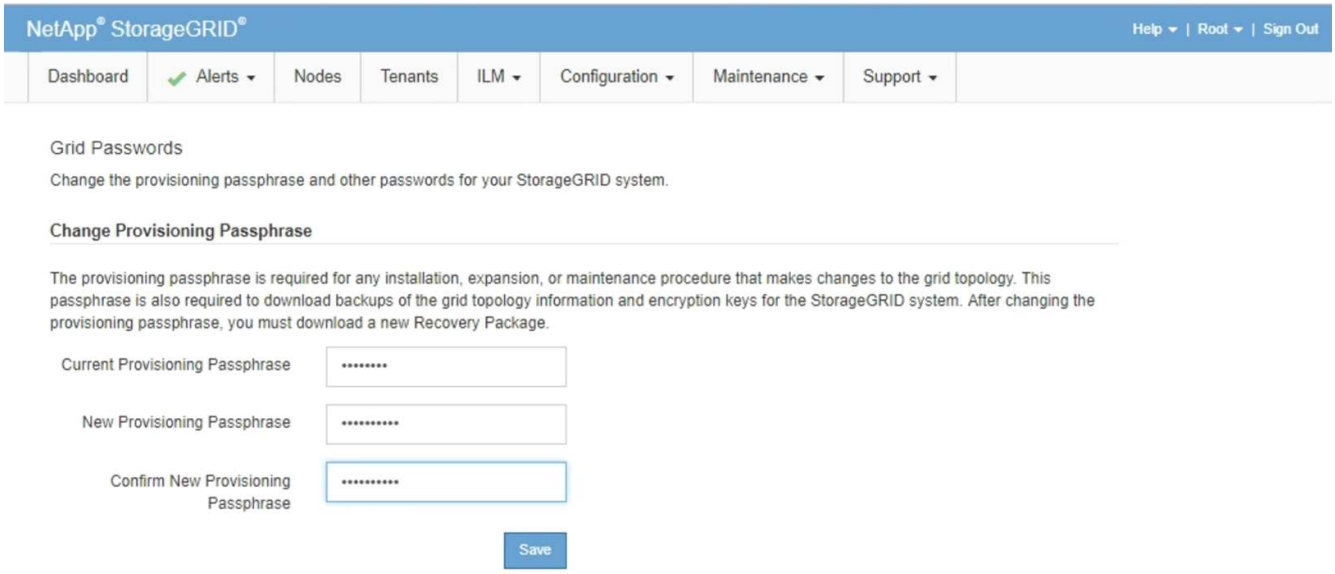
- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須擁有維護或根存取權限。
- 您必須擁有目前的資源配置通關密碼。

關於這項工作

許多安裝與維護程序、以及下載恢復套件時、都需要使用資源配置密碼。中未列出資源配置通關密碼 `Passwords.txt` 檔案：請務必記錄資源配置通關密碼、並將密碼保存在安全的位置。

步驟

1. 選擇*組態*>*存取控制*>*網格密碼*。

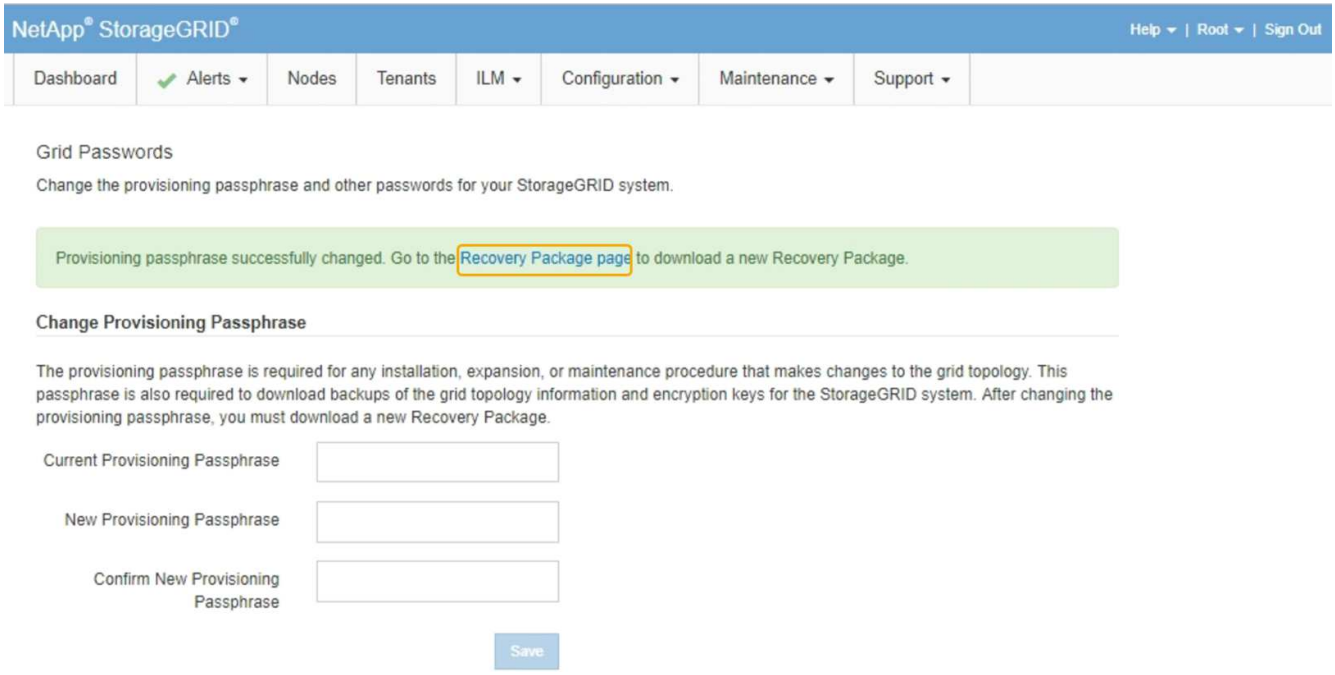


2. 輸入您目前的資源配置通關密碼。
3. 輸入新密碼。密碼必須包含至少8個字元、且不得超過32個字元。密碼區分大小寫。

   將新的資源配置通關密碼儲存在安全的位置。安裝、擴充和維護程序都必須如此。

4. 重新輸入新的通關密碼、然後按一下「儲存」。

   資源配置通關密碼變更完成時、系統會顯示綠色的成功標語。變更應在一分鐘內完成。



5. 選取成功橫幅內的*恢復套件頁面*連結。
6. 從Grid Manager下載新的恢復套件。選擇*維護*>*恢復套件*、然後輸入新的資源配置通關密碼。

> 變更資源配置通關密碼之後、您必須立即下載新的恢復套件。恢復套件檔案可讓您在發生故障時還原系統。

變更瀏覽器工作階段逾時

您可以控制Grid Manager和Tenant Manager使用者是否在超過一定時間內處於非作用中狀態時登出。

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

GUI無活動逾時預設為900秒（15分鐘）。如果使用者的瀏覽器工作階段在這段時間內未處於作用中狀態、工作階段就會逾時。

視需要、您可以設定GUI無活動逾時顯示選項來增加或減少逾時期間。

如果啟用單一登入（SSO）且使用者的瀏覽器工作階段逾時、系統的運作方式就如同使用者手動按下*登出*。使用者必須重新輸入SSO認證資料、StorageGRID 才能再次存取功能。

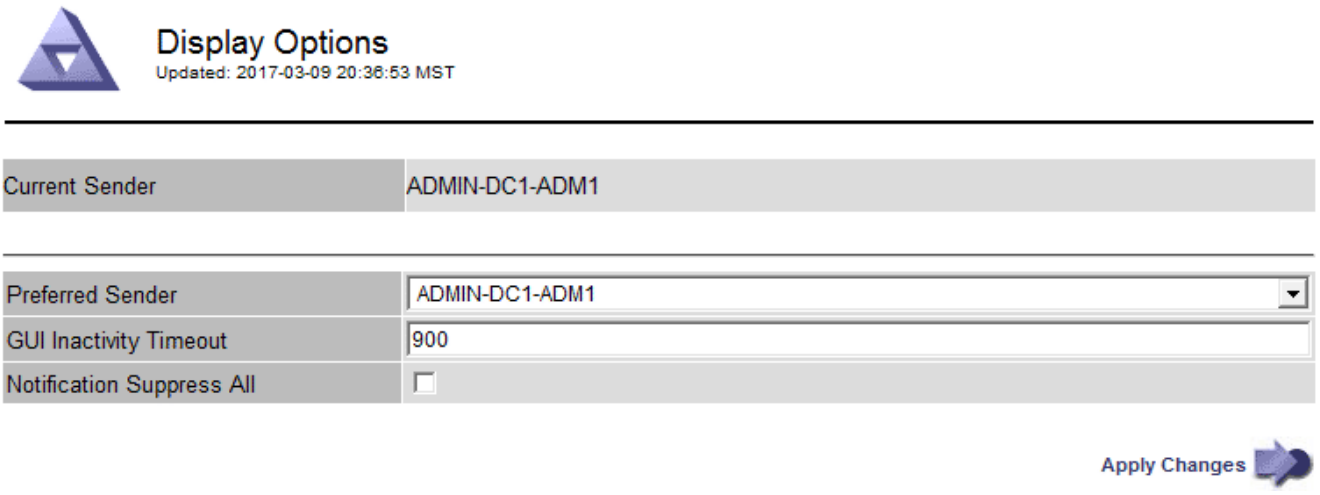
使用者工作階段逾時也可由下列項目控制：

- 另有一個不可設定StorageGRID 的獨立式計時功能、可用於系統安全性。根據預設、每個使用者的驗證權杖會在使用者登入後16小時過期。當使用者的驗證過期時、即使未達到GUI閒置逾時的值、該使用者仍會自動登出。若要續約權杖、使用者必須重新登入。
- 身分識別供應商的逾時設定、假設啟用SSO StorageGRID 以供執行功能。

步驟

1. 選擇*組態*>*系統設定*>*顯示選項*。
2. 若為* GUI無活動逾時*、請輸入60秒以上的逾時期間。

   如果您不想使用此功能、請將此欄位設為0。使用者登入後16小時內即會登出、驗證權杖即過期。



3. 按一下*套用變更*。

   新設定不會影響目前登入的使用者。使用者必須重新登入或重新整理瀏覽器、新的逾時設定才會生效。

相關資訊

"單一登入的運作方式"

"使用租戶帳戶"

檢視StorageGRID 功能介紹資訊

您可以視StorageGRID 需要檢視您的支援資訊、例如網格的最大儲存容量。

您需要的產品

- 您必須使用支援的瀏覽器登入Grid Manager。

關於這項工作

如果StorageGRID 此款作業系統的軟體授權發生問題、儀表板上的「健全狀況」面板會顯示「授權狀態」圖示和*授權*連結。此數字表示有多少與授權相關的問題。

步驟

若要檢視授權、請執行下列其中一項：

- 在儀表板的健全狀況面板中、按一下授權狀態圖示或*授權*連結。僅當授權發生問題時、才會顯示此連結。
- 選擇*維護*系統*授權。

此時會出現「授權」頁面、並提供下列有關目前授權的唯讀資訊：

- 系統ID、這是此安裝的唯一識別號碼StorageGRID StorageGRID
- 授權序號
- 網格的授權儲存容量
- 軟體授權結束日期
- 支援服務合約結束日期
- 授權文字檔的內容

若為StorageGRID 在發行版本不含於Es11的授權、授權儲存容量將不包含在授權檔案中、並會顯示「請參閱授權合約」訊息、而非數值。

更新StorageGRID 版的更新版的授權資訊

您必須在StorageGRID 授權條款變更時、隨時更新您的不適用系統的授權資訊。例如、如果您為網格購買額外的儲存容量、則必須更新授權資訊。

您需要的產品

- 您必須有新的授權檔案才能套用StorageGRID 到您的系統。
- 您必須擁有特定的存取權限。
- 您必須擁有資源配置通關密碼。

步驟

1. 選擇*維護*系統*授權。

2. 在StorageGRID * Provisioning Passphrase *（*配置密碼）文字方塊中、輸入您的供應系統的密碼。
3. 按一下*瀏覽*。
4. 在「開啟」對話方塊中、找出並選取新的授權檔案 (`.txt`）、然後按一下*「Open*（開啟*）」。

   系統會驗證並顯示新的授權檔案。

5. 按一下「 * 儲存 * 」。

使用Grid Management API

您可以使用Grid Management REST API而非Grid Manager使用者介面來執行系統管理工作。例如、您可能想要使用API來自動化作業、或更快建立多個實體、例如使用者。

Grid Management API使用Swagger開放原始碼API平台。Swagger提供直覺式使用者介面、可讓開發人員和非開發人員StorageGRID 利用API在Real-Time中執行作業。

頂級資源

Grid Management API提供下列頂級資源：

- `/grid`：只有Grid Manager使用者才能存取、而且是根據已設定的群組權限而定。
- `/org`：只有屬於租戶帳戶的本機或聯盟LDAP群組的使用者才能存取。如需詳細資訊、請參閱使用租戶帳戶的相關資訊。
- `/private`：只有Grid Manager使用者才能存取、而且是根據已設定的群組權限而定。這些API僅供內部使用、並未公開記錄。這些API也可能隨時變更、恕不另行通知。

相關資訊

"使用租戶帳戶"

"Prometheus：查詢基礎"

網格管理**API**作業

Grid Management API會將可用的API作業組織到下列各節。

- 帳戶：管理儲存租戶帳戶的作業、包括建立新帳戶及擷取特定帳戶的儲存使用量。
- 警示：列出目前警示（舊系統）的作業、並傳回有關網格健全狀況的資訊、包括目前警示和節點連線狀態摘要。
- 警示歷史記錄-已解決警示的作業。
- 警示接收器-警示通知接收器（電子郵件）上的作業。
- 警示規則-警示規則上的作業。
- 警示靜音-警示靜音作業。
- 警示：警示操作。
- 稽核-列出及更新稽核組態的作業。

- 驗證：執行使用者工作階段驗證的作業。

  Grid Management API支援承載權杖驗證方案。若要登入、您必須在驗證要求的Json實體中提供使用者名稱和密碼（也就是 `POST /api/v3/authorize`）。如果使用者已成功驗證、則會傳回安全性權杖。此權杖必須在後續API要求的標頭中提供（「授權：bear_tokon_」）。

  > 如果StorageGRID 啟用了單一登入功能、您必須執行不同的驗證步驟。請參閱「若啟用單一登入、則驗證API」。

  請參閱「防範跨網站要求偽造」、以取得改善驗證安全性的資訊。

- 用戶端-憑證-作業設定用戶端憑證、以便StorageGRID 使用外部監控工具安全存取。
- 組態-與Grid Management API產品版本相關的作業。您可以列出該版本所支援的產品版本和Grid Management API主要版本、也可以停用已過時的API版本。
- 停用功能-檢視可能已停用之功能的作業。
- * DNS伺服器*：列出及變更已設定外部DNS伺服器的作業。
- 端點-網域名稱-列出及變更端點網域名稱的作業。
- 銷毀編碼-刪除編碼設定檔的作業。
- 擴充：擴充作業（程序層級）。
- 擴充節點-擴充作業（節點層級）。
- 擴充站台-擴充作業（站台層級）。
- 網格網路-列出及變更網格網路清單的作業。
- 網格密碼-網格密碼管理作業。
- 群組：管理本機Grid系統管理員群組的作業、以及從外部LDAP伺服器擷取聯盟Grid系統管理員群組。
- 身分識別來源-作業：設定外部身分識別來源、以及手動同步處理聯盟群組與使用者資訊。
- * ILM *-資訊生命週期管理（ILM）的營運。
- 授權-擷取StorageGRID 及更新此功能的作業。
- 記錄：收集及下載記錄檔的作業。
- 指標：StorageGRID 針對包括即時度量查詢在單一時間點進行的運算、以及在一段時間內進行的範圍度量查詢。Grid Management API使用Prometheus系統監控工具作為後端資料來源。如需建構Prometheus查詢的相關資訊、請參閱Prometheus網站。

  > 包括的指標*`private`* 其名稱僅供內部使用。這些指標可能會在StorageGRID 不另行通知的情況下於各個版本之間變更。

- 節點健全狀況-節點健全狀況狀態的作業。
- * ntp伺服器*-列出或更新外部網路時間傳輸協定（NTP）伺服器的作業。
- 物件-物件和物件中繼資料的作業。
- 恢復-恢復程序的作業。
- 恢復套件-下載恢復套件的作業。

- 地區-檢視及建立區域的作業。
- * S3物件鎖定*-全域S3物件鎖定設定的作業。
- 伺服器認證-檢視及更新Grid Manager伺服器認證的作業。
- * SNMP *-目前SNMP組態上的作業。
- 流量類別-流量分類原則的作業。
- 不受信任的用戶端網路：不受信任的用戶端網路組態上的作業。
- 使用者-檢視及管理Grid Manager使用者的作業。

發出**API**要求

Swagger使用者介面提供每個API作業的完整詳細資料和文件。

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。

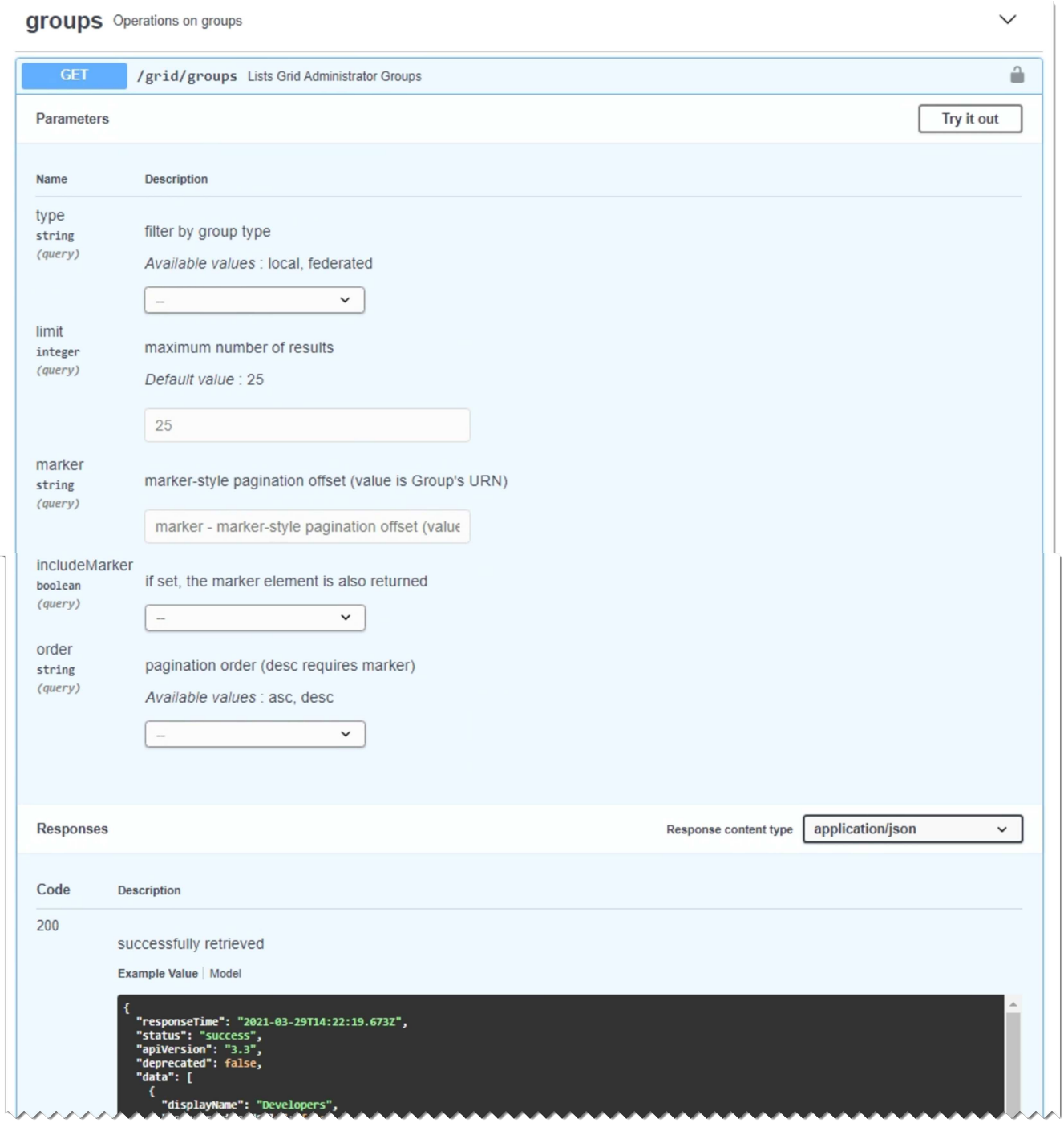
> 您使用API文件網頁執行的任何API作業都是即時作業。請小心不要錯誤地建立、更新或刪除組態資料或其他資料。

步驟

1. 從Grid Manager標頭中選擇* Help*>* API Documentation *。
2. 選取所需的作業。

   展開API作業時、您可以看到可用的HTTP動作、例如GET、PUT、update和DELETE。

3. 選取HTTP動作以查看申請詳細資料、包括端點URL、任何必要或選用參數的清單、申請本文的範例（視需要）、以及可能的回應。



4. 判斷要求是否需要其他參數、例如群組或使用者ID。然後取得這些值。您可能需要先發出不同的API要求、才能取得所需的資訊。
5. 判斷您是否需要修改範例要求本文。如果是、您可以按一下*模型*來瞭解每個欄位的需求。
6. 按一下*試用*。
7. 提供任何必要的參數、或視需要修改申請本文。
8. 按一下*執行*。
9. 檢閱回應代碼以判斷要求是否成功。

Grid Management API版本管理

Grid Management API使用版本管理來支援不中斷營運的升級。

例如、此Request URL會指定API版本3。

```
https://hostname_or_ip_address/api/v3/authorize
```

當進行*不相容*的變更時、會使租戶管理API的主要版本與舊版相容。當做出*與舊版相容*的變更時、租戶管理API的次要版本會被提升。相容的變更包括新增端點或新屬性。下列範例說明如何根據所做的變更類型來提高API版本。

API變更類型	舊版本	新版本
與舊版相容	2.1	2.2
與舊版不相容	2.1	3.0

第一次安裝StorageGRID 時、只會啟用最新版本的Grid Management API。不過、當您升級StorageGRID 至全新的功能版本的更新版時、您仍可繼續存取舊版的API、以取得至少一個StorageGRID 版本的更新功能。

> 您可以使用Grid Management API來設定支援的版本。如需詳細資訊、請參閱Swagger API文件的「config」一節。您應該在更新所有Grid Management API用戶端以使用較新版本之後、停用對較舊版本的支援。

過時的要求會以下列方式標示為已過時：

- 回應標頭為「deprecated：true」
- Json回應本文包含「deprecated」：true
- NMS.log中會新增已過時的警告。例如：

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

判斷目前版本支援哪些API版本

使用下列API要求傳回支援的API主要版本清單：

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

指定要求的**API**版本

您可以使用路徑參數來指定API版本 (`/api/v3`）或標頭 (`Api-Version: 3`）。如果您同時提供這兩個值、則標頭值會覆寫路徑值。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

防範跨網站要求偽造（**CSRF**）

您StorageGRID 可以使用CSRF權杖來強化使用Cookie的驗證功能、協助防範跨網站要求偽造（CSRF）攻擊。Grid Manager與租戶管理程式會自動啟用此安全功能、其他API用戶端則可選擇是否在登入時啟用。

攻擊者若能觸發要求至不同網站（例如HTTP表單POST）、可能會導致使用登入使用者的Cookie發出特定要求。

利用CSRF權杖協助防範CSRF攻擊。StorageGRID啟用時、特定Cookie的內容必須符合特定標頭或特定POST本文參數的內容。

若要啟用此功能、請設定 `csrfToken` 參數至 `true` 驗證期間。預設值為 `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果正確、則為A `GridCsrfToken` Cookie是以隨機值設定、用於登入Grid Manager和 `AccountCsrfToken` Cookie是以隨機值設定、用於登入租戶管理程式。

如果Cookie存在、則所有可修改系統狀態的要求（POST、PUT、PATCH、DELETE）都必須包含下列其中一項：

- 。 `X-Csrf-Token` 標頭、並將標頭值設為CSRF權杖Cookie的值。
- 對於接受格式編碼實體的端點：a `csrfToken` 表單編碼要求本文參數。

如需其他範例與詳細資料、請參閱線上API文件。

> 具有CSRF權杖Cookie集的要求也會強制執行 `"Content-Type: application/json"` 任何要求的標頭、如果要求Json要求實體做為額外的CSRF攻擊防護、

如果啟用單一登入、請使用**API**

如果StorageGRID 您的系統已啟用單一登入（SSO）、則無法使用標準驗證API要求登入及登出Grid Management API或租戶管理API。

如果啟用單一登入、請登入**API**

如果已啟用單一登入（SSO）、您必須發出一系列API要求、才能從適用於Grid Management API或租戶管理API的AD FS取得驗證權杖。

您需要的產品

- 您知道屬於StorageGRID 某個位向使用者群組的聯盟使用者的SSO使用者名稱和密碼。
- 如果您想要存取租戶管理API、就知道租戶帳戶ID。

關於這項工作

若要取得驗證權杖、您可以使用下列其中一個範例：

- 。 `storagegrid-ssoauth.py` Python指令碼、位於StorageGRID 安裝檔案目錄中 (`./rpms` 適用於Red Hat Enterprise Linux或CentOS、 `./debs` 適用於Ubuntu或DEBIAN,以及 `./vsphere` （適用於VMware）。
- Curl要求的工作流程範例。

  如果執行速度太慢、捲曲工作流程可能會逾時。您可能會看到以下錯誤：在此回應中找不到有效的SubjectConfirmation。

  > 範例Curl工作流程無法防止其他使用者看到密碼。

如果您遇到URL編碼問題、可能會看到以下錯誤：不支援的SAML版本。

步驟

1. 選取下列方法之一以取得驗證權杖：
   - 使用 `storagegrid-ssoauth.py` Python指令碼：前往步驟2。
   - 使用Curl要求。前往步驟3。
2. 如果您要使用 `storagegrid-ssoauth.py` 指令碼、將指令碼傳遞給Python解釋器、然後執行指令碼。

出現提示時、請輸入下列引數的值：

- SSO使用者名稱
- 安裝了鏡面的網域StorageGRID
- 解決這個StorageGRID 問題
- 若要存取租戶管理API、請輸入租戶帳戶ID。

+

輸出中提供了驗證權杖。StorageGRID您現在可以將權杖用於其他要求、類似於未使用SSO時使用API的方式。

3. 如果您要使用捲髮要求、請使用下列程序。

   a. 宣告登入所需的變數。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

   若要存取Grid Management API、請使用0做為 `TENANTACCOUNTID`。

   b. 若要接收已簽署的驗證URL、請向發出POST要求 `/api/v3/authorize-saml`，並從回應中移除其他Json編碼。

   此範例顯示的已簽署驗證URL的POST要求 `TENANTACCOUNTID`。結果會傳遞至python -m json.tool以移除Json編碼。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

此範例的回應包含URL編碼的已簽署URL、但不包含其他JSON-encoding層。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 儲存 `SAMLRequest` 從回應中取得以供後續命令使用。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. 取得完整的URL、其中包含AD FS的用戶端要求ID。

其中一個選項是使用先前回應的URL來要求登入表單。

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

回應包括用戶端要求ID：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 從回應中儲存用戶端要求ID。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 將您的認證資料傳送至先前回應的表單動作。

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=For
msAuthentication" --include
```

AD FS會傳回302重新導向、並在標頭中顯示其他資訊。

> 如果您的SSO系統已啟用多因素驗證（MFA）、則表單POST也會包含第二個密碼或其他認證資料。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 儲存 `MSISAuth` 來自回應的Cookie。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 從驗證貼文傳送內含Cookie的Get要求至指定位置。

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --cookie "MSISAuth=$MSISAuth" --include
```

回應標頭會包含AD FS工作階段資訊、以供日後登出使用、而回應本文會在隱藏表單欄位中包含SAMLResponse。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 儲存 `SAMLResponse` 從隱藏欄位：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用儲存的 `SAMLResponse`、打造StorageGRID 一個不一樣的`/api/saml-response` 要求產生StorageGRID 驗證權杖。

適用於 `RelayState`、如果您要登入Grid Management API、請使用租戶帳戶ID或使用0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

回應包括驗證權杖。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 將回應中的驗證權杖另存為 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

您現在可以使用 `MYTOKEN` 對於其他要求、類似於不使用SSO時使用API的方式。

如果啟用單一登入、則登出API

如果已啟用單一登入（SSO）、您必須發出一系列API要求、以登出Grid Management API或租戶管理API。

關於這項工作

如有需要、StorageGRID 只要從貴組織的單一登出頁面登出、即可登出此功能。或者、您也可以觸發StorageGRID 來自下列項目的單一登出（SLO）：需要有效StorageGRID 的SESO承載權杖。

步驟

1. 若要產生已簽署的登出要求、請通過 `cookie "sso=true"` 至SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

會傳回登出URL：

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 儲存登出URL。

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

3. 傳送要求至登出URL以觸發SLO並重新導向StorageGRID 至還原。

```
curl --include "$LOGOUT_REQUEST"
```

會傳回302回應。重新導向位置不適用於純API登出。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. 刪除StorageGRID 不記名權杖。

刪除StorageGRID 此不含SSO的不含支援權杖的方式相同。如果 `cookie "sso=true"` 未提供、使用者登出StorageGRID 時不會影響SSO狀態。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

答 `204 No Content` 回應表示使用者現在已登出。

```
HTTP/1.1 204 No Content
```

使用StorageGRID 資訊安全認證

安全證書是小型資料檔案、用於在StorageGRID 各個元件之間、StorageGRID 以及在各個元件與外部系統之間建立安全且值得信賴的連線。

使用兩種類型的安全性憑證：StorageGRID

- 使用**HTTPS**連線時需要伺服器憑證。伺服器憑證用於在用戶端和伺服器之間建立安全連線、驗證伺服器的用戶端身分、並提供安全的資料通訊路徑。伺服器和用戶端各有一份憑證複本。
- *用戶端憑證*驗證伺服器的用戶端或使用者身分、提供比僅密碼更安全的驗證。用戶端憑證不會加密資料。

當用戶端使用HTTPS連線至伺服器時、伺服器會以含有公開金鑰的伺服器憑證回應。用戶端會將伺服器簽章與憑證複本上的簽章進行比較、藉此驗證此憑證。如果簽名相符、用戶端會使用相同的公開金鑰啟動與伺服器的工作階段。

充當某些連線（例如負載平衡器端點）的伺服器、或作為其他連線（例如CloudMirror複寫服務）的用戶端。StorageGRID

外部憑證授權單位（CA）可核發完全符合組織資訊安全原則的自訂憑證。此外、還包括內建的憑證授權單位（CA）、可在系統安裝期間產生內部CA憑證StorageGRID 。根據預設、這些內部CA憑證是用來保護內部StorageGRID 的不穩定流量。雖然您可以將內部CA憑證用於非正式作業環境、但正式作業環境的最佳做法是使用外部憑證授權單位所簽署的自訂憑證。不具證書的不安全連線也受到支援、但不建議使用。

- 自訂CA憑證不會移除內部憑證；不過、自訂憑證應該是為驗證伺服器連線所指定的憑證。
- 所有自訂憑證都必須符合伺服器憑證的系統強化準則。

  "系統強化"

- 支援將CA的憑證整合至單一檔案（稱為CA憑證套件）StorageGRID 。

> 此外、還包括所有網格上相同的作業系統CA憑證。StorageGRID在正式作業環境中、請務必指定由外部憑證授權單位簽署的自訂憑證、以取代作業系統CA憑證。

伺服器和用戶端憑證類型的變種會以多種方式實作。在設定系統之前、您應該StorageGRID 準備好特定的支援功能組態所需的所有憑證。

憑證	憑證類型	說明	導覽位置	詳細資料
系統管理員用戶端憑證	用戶端	安裝在每個用戶端上、StorageGRID 讓功能驗證外部用戶端存取。 • 允許授權的外部用戶端存取StorageGRID 《The WilsPrometheus資料庫》。 • 允許StorageGRID 使用外部工具安全監控功能。	組態>*存取控制*>*用戶端憑證*	"設定系統管理員用戶端憑證"

憑證	憑證類型	說明	導覽位置	詳細資料
身分識別聯盟憑證	伺服器	驗證StorageGRID Reality與外部Active Directory、OpenLDAP或Oracle Directory Server之間的連線。用於身分識別聯盟、可讓管理員群組和使用者由外部系統管理。	組態>*存取控制*>*身分識別聯盟*	"使用身分識別聯盟"
單一登入（SSO）憑證	伺服器	驗證Active Directory Federation Services（AD FS）與StorageGRID 用於單一登入（SSO）要求的功能之間的連線。	組態>*存取控制*>*單一登入*	"設定單一登入"
金鑰管理伺服器（KMS）憑證	伺服器與用戶端	驗證StorageGRID 支援功能與外部金鑰管理伺服器（KMS）之間的連線、此伺服器可為StorageGRID 應用裝置節點提供加密金鑰。	組態>*系統設定*>*金鑰管理伺服器*	"新增金鑰管理伺服器（KMS）"
電子郵件警示通知憑證	伺服器與用戶端	驗證用於StorageGRID 警示通知的SMTP電子郵件伺服器與功能鏈之間的連線。 • 如果與SMTP伺服器的通訊需要傳輸層安全性（TLS）、您必須指定電子郵件伺服器CA憑證。 • 只有在SMTP電子郵件伺服器需要用戶端憑證進行驗證時、才指定用戶端憑證。	警示>*電子郵件設定*	"監控安培；疑難排解"

憑證	憑證類型	說明	導覽位置	詳細資料
負載平衡器端點憑證	伺服器	驗證S3或Swift用戶端之間的連線、以及StorageGRID 閘道節點或管理節點上的「SSecure Load Balancer」服務。當您設定負載平衡器端點時、您可以上傳或產生負載平衡器憑證。用戶端應用程式在連線StorageGRID至時、會使用負載平衡器憑證來儲存及擷取物件資料。 *附註：*負載平衡器憑證是正常StorageGRID 執行過程中最常使用的憑證。	組態>*網路設定*>*負載平衡器端點*	• "設定負載平衡器端點" • 建立FabricPool負載平衡器端點以利執行 "設定StorageGRID適用於FabricPool 靜態的"
管理介面伺服器憑證	伺服器	驗證用戶端網頁瀏覽器與StorageGRID RealSet管理介面之間的連線、讓使用者能夠存取Grid Manager和Tenant Manager、而不會出現安全性警告。 此憑證也會驗證Grid Management API和租戶管理API連線。 您可以使用內部CA憑證或上傳自訂憑證。	組態>*網路設定*>*伺服器憑證*	• "設定伺服器憑證" • "為Grid Manager和Tenant Manager設定自訂伺服器憑證"
雲端儲存資源池端點憑證	伺服器	驗證StorageGRID從「支援不支援的雲端儲存資源池」到外部儲存位置（例如S3 Glacier或Microsoft Azure Blob儲存設備）的連線。每種雲端供應商類型都需要不同的憑證。	• ILM >*儲存資源池	"使用ILM管理物件"

憑證	憑證類型	說明	導覽位置	詳細資料
平台服務端點憑證	伺服器	驗證StorageGRID 從SReals功能 平台服務到S3儲存資源的連線。	租戶管理程式>*儲存設備（S3）>*平台服務端點	"使用租戶帳戶"
物件儲存API服務端點伺服器憑證	伺服器	驗證安全S3或Swift用戶端連線至儲存節點上的本機發佈路由器（LDR）服務、或閘道節點上已過時的連線負載平衡器（CLB）服務。	組態>*網路設定*>*負載平衡器端點*	"設定自訂伺服器憑證、以連線至儲存節點或CLB服務"

範例**1**：負載平衡器服務

在此範例中StorageGRID 、用作伺服器的是功能。

1. 您可以設定負載平衡器端點、並在StorageGRID 中上傳或產生伺服器憑證。
2. 您可以設定S3或Swift用戶端連線至負載平衡器端點、然後將相同的憑證上傳至用戶端。
3. 當用戶端想要儲存或擷取資料時、會使用HTTPS連線至負載平衡器端點。
4. 以伺服器憑證做出回應、其中包含公開金鑰、並以私密金鑰為基礎提供簽名。StorageGRID
5. 用戶端會將伺服器簽章與憑證複本上的簽章進行比較、藉此驗證此憑證。如果簽名相符、用戶端就會使用相同的公開金鑰來啟動工作階段。
6. 用戶端會將物件資料傳送StorageGRID 至物件資料。

範例**2**：外部金鑰管理伺服器（**KMS**）

在此範例中StorageGRID 、由客戶扮演的角色就是

1. 使用外部金鑰管理伺服器軟體、您可以將StorageGRID 效能設定為KMS用戶端、並取得CA簽署的伺服器憑證、公用用戶端憑證及用戶端憑證的私密金鑰。
2. 您可以使用Grid Manager設定KMS伺服器、並上傳伺服器和用戶端憑證及用戶端私密金鑰。
3. 當某個節點需要加密金鑰時、它會向KMS伺服器提出要求、要求其中包含來自憑證的資料、以及以私密金鑰為基礎的簽名。StorageGRID
4. KMS伺服器會驗證憑證簽章、並決定其是否值得信賴StorageGRID 。
5. KMS伺服器會使用已驗證的連線來回應。