



使用**Grid Management API**

StorageGRID 11.5

NetApp
April 11, 2024

目錄

使用Grid Management API	1
頂級資源	1
網格管理API作業	1
發出API要求	3
Grid Management API版本管理	5
防範跨網站要求偽造 (CSRF)	6
如果啟用單一登入、請使用API	7

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_token_」）。



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。

GET /grid/groups Lists Grid Administrator Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated <input type="text" value="--"/>
limit integer (query)	maximum number of results Default value : 25 <input type="text" value="25"/>
marker string (query)	marker-style pagination offset (value is Group's URN) <input type="text" value="marker - marker-style pagination offset (value"/>
includeMarker boolean (query)	if set, the marker element is also returned <input type="text" value="--"/>
order string (query)	pagination order (desc requires marker) Available values : asc, desc <input type="text" value="--"/>

Responses Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers",</pre>

4. 判斷要求是否需要其他參數、例如群組或使用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。

```
python3 /tmp/storagegrid-ssoauth.py
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****
*****
StorageGRID Auth Token: 56e07bf-21f6-40b7-afob-5c6cacfb25e7
```

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...
sS1%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...sS1%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=fZHRTOMwFIZfzb...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=fZHRTomwFIZfhh...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。


```
{
  "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入頁面登出、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入（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://ads.example.com/ads/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "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=fZDNboMwEIRfhZ...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: MSISignoutProtocol=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
```

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。