如果啟用單一登入、請使用API StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-116/admin/use-api-if-sso-is-enabled-adfs.html on October 03, 2025. Always check docs.netapp.com for the latest.

目錄

如果啟用單一登入、請使用API . . . 1
如果啟用單一登入、請使用API（Active Directory） . . . 1
如果啟用單一登入、請登入API . . . 1
如果啟用單一登入、請登出API . . . 6
如果啟用單一登入、請使用API（Azure） . . . 7
如果啟用Azure單一登入、請登入API . . . 7
如果啟用單一登入、請使用API（PingFedate） . . . 9
如果啟用單一登入、請登入API . . . 9
如果啟用單一登入、請登出API . . . 12

如果啟用單一登入、請使用API

如果啟用單一登入、請使用API（Active Directory）

如果您有 已設定並啟用單一登入（SSO） 而且您使用Active Directory做為SSO供應商、必須發出一系列API要求、才能取得適用於Grid Management API或租戶管理API的驗證權杖。

如果啟用單一登入、請登入API

如果您使用Active Directory做為SSO身分識別供應商、則適用這些指示。

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：

- "storagegride-ssoauth.py" Python指令碼、位於StorageGRID 下列目錄中：安裝檔案目錄（如Red Hat Enterprise Linux或CentOS、Ubuntu或DEBIANS的"./rpms"、VMware的"./vSphere."）。
- 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、可能會看到錯誤：「Unsupported SAML version（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 sosoauth.py" Python指令碼。前往步驟2。
   - 使用Curl要求。前往步驟3。
2. 如果要使用"storagegrid ssoauth.py"指令碼、請將指令碼傳遞給Python解譯程式、然後執行指令碼。

   出現提示時、請輸入下列引數的值：
   - SSO方法。輸入「ADFS」或「ADFS」。
   - SSO使用者名稱
   - 安裝了鏡面的網域StorageGRID
   - 解決這個StorageGRID 問題
   - 租戶帳戶ID（如果您要存取租戶管理API）。

```
python3 storagegrid-ssoauth.py
sso_method: adfs
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: 56eb07bf-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作為「TENANTACCOUNTID」。

   b. 若要接收已簽署的驗證URL、請向「/API/v3/授權-SAML」發出POST要求、並從回應中移除其他Json編碼。

   此範例顯示「TENANTACCOUNTID」的已簽署驗證URL的POST要求。結果將傳送至「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. 從回應中儲存「AMLRequest」、以便在後續命令中使用。

```
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=FormsAuthentication" --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. 從回應中儲存「ISAUTH」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. 從隱藏欄位儲存「AMLResponse"：

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

j. 使用儲存的「AMLResponse"（AMLResponse"）、提出StorageGRID（/API/SAML-Response"）要求、以產生StorageGRID 一個反映驗證權杖。

若為「RelayState」、請使用租戶帳戶ID、若您想登入Grid Management API、請使用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儲存為「MoYTOKEN」。

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

您現在可以將「MoYTOKEN」用於其他要求、類似於不使用SSO時使用API的方式。

如果啟用單一登入、請登出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。如果您使用Active Directory做為SSO身分識別供應商、則適用這些指示

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、請將「Cookie "SSO=true"」傳遞給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=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: 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。如果未提供「Cookie "SSO = true」、使用者將登出StorageGRID 、而不會影響SSO狀態。

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

「204無內容」回應表示使用者現在已登出。

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

如果啟用單一登入、請使用API（Azure）

如果您有 已設定並啟用單一登入（SSO） 您可以使用Azure做為SSO供應商、使用兩個範例指令碼來取得適用於Grid Management API或租戶管理API的驗證權杖。

如果啟用Azure單一登入、請登入API

如果您使用Azure做為SSO身分識別供應商、則適用這些指示

您需要的產品

- 您知道屬於StorageGRID 某個支援對象群組的聯盟使用者的SSO電子郵件地址和密碼。
- 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、您可以使用下列範例指令碼：

- "storagegRide-ssoauth-azure.py" Python指令碼
- "storagegRide-ssoauth-azure.js" Node.js指令碼

這兩個指令碼都位於StorageGRID 支援Red Hat Enterprise Linux或CentOS的版本/rpmss目錄（適用於Ubuntu或DEBIANS的版本/debs目錄、以及適用於VMware的版本/vSphere目錄）。

若要寫入您自己與Azure的API整合、請參閱「storagegRide-ssoauth-azure.py」指令碼。Python指令碼會StorageGRID 直接提出兩項要求（先取得SAMLRequest、之後取得授權權杖）、也會呼叫Node.js指令碼與Azure互動、以執行SSO作業。

SSO作業可以使用一系列API要求執行、但這樣做並不直接。Puppeteer Node.js模組可用來掃描Azure SSO介面。

如果您遇到URL編碼問題、可能會看到錯誤：「Unsupported SAML version（不支援的SAML版本）」。

步驟

1. 安裝所需的相依性、如下所示：
   a. 安裝Node.js（請參閱 "https://nodejs.org/en/download/"）。
   b. 安裝所需的Node.js模組（puppeteer和jsdom）：

      "npPM install -g <module>

2. 將Python指令碼傳遞給Python解譯器以執行指令碼。

   然後Python指令碼會呼叫對應的Node.js指令碼、以執行Azure SSO互動。

3. 出現提示時、請輸入下列引數的值（或使用參數傳入）：
   - 用於登入Azure的SSO電子郵件地址
   - 解決這個StorageGRID 問題
   - 租戶帳戶ID（如果您要存取租戶管理API）
4. 出現提示時、請輸入密碼、並在需要時準備好提供MFA授權給Azure。

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

指令碼假設MFA是使用Microsoft驗證者完成。您可能需要修改指令碼、以支援其他形式的MFA（例如輸入透過文字訊息接收的程式碼）。

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。

如果啟用單一登入、請使用API（PingFedate）

如果您有 已設定並啟用單一登入（SSO） 而且您使用PingFedate做為SSO供應商、必須發出一系列API要求、才能取得適用於Grid Management API或租戶管理API的驗證權杖。

如果啟用單一登入、請登入API

如果您使用PingFedate做為SSO身分識別供應商、則適用這些指示

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：

- "storagegride-ssoauth.py" Python指令碼、位於StorageGRID 下列目錄中：安裝檔案目錄（如Red Hat Enterprise Linux或CentOS、Ubuntu或DEBIANS的"./rpms"、VMware的"./vSphere."）。
- 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、可能會看到錯誤：「Unsupported SAML version（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 sosoauth.py" Python指令碼。前往步驟2。
   - 使用Curl要求。前往步驟3。
2. 如果要使用"storagegrid ssoauth.py"指令碼、請將指令碼傳遞給Python解譯程式、然後執行指令碼。

   出現提示時、請輸入下列引數的值：
   - SSO方法。您可以輸入「pingfederate」（Pingfederate、pingfederate等）的任何變化。
   - SSO使用者名稱
   - 安裝了鏡面的網域StorageGRID 。此欄位不適用於PingFedate。您可以將其保留空白或輸入任何值。

- 解決這個StorageGRID 問題
- 租戶帳戶ID（如果您要存取租戶管理API）。

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-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 TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

   若要存取Grid Management API、請使用0作為「TENANTACCOUNTID」。

   b. 若要接收已簽署的驗證URL、請向「/API/v3/授權-SAML」發出POST要求、並從回應中移除其他Json編碼。

   此範例顯示TENANTACCOUNTID的簽署驗證URL的POST要求。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://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 從回應中儲存「AMLRequest」、以便在後續命令中使用。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 匯出回應和Cookie、並回應回應回應：

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 匯出「pf.adaperId」值、並回應回應回應：

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 匯出「Ha」值（移除結尾斜槓/）、然後回應回應：

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 匯出「行動」值：

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 傳送內含認證的Cookie：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 從隱藏欄位儲存「AMLResponse"：

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

j. 使用儲存的「AMLResponse"（AMLResponse"）、提出StorageGRID（/API/SAML-Response"）要求、以產生StorageGRID 一個反映驗證權杖。

若為「RelayState」、請使用租戶帳戶ID、若您想登入Grid Management API、請使用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儲存為「MoYTOKEN」。

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

您現在可以將「MoYTOKEN」用於其他要求、類似於不使用SSO時使用API的方式。

如果啟用單一登入、請登出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。如果您使用PingFedate做為SSO身分識別供應商、則適用這些指示

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、請將「Cookie "SSO=true"」傳遞給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://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. 儲存登出URL。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?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: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

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。如果未提供「Cookie "SSO = true」、使用者將登出StorageGRID 、而不會影響SSO狀態。

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

「204無內容」回應表示使用者現在已登出。

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

版權資訊

Copyright © 2025 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。