



# 使用安全性追蹤來驗證存取 ONTAP 9

NetApp  
April 24, 2024

# 目錄

|                      |    |
|----------------------|----|
| 使用安全性追蹤來驗證存取 .....   | 1  |
| 安全追蹤的運作方式 .....      | 1  |
| 存取類型會檢查監控的安全追蹤 ..... | 1  |
| 建立安全追蹤時的考量 .....     | 2  |
| 執行安全追蹤 .....         | 2  |
| 解讀安全性追蹤結果 .....      | 10 |
| 何處可找到其他資訊 .....      | 11 |

# 使用安全性追蹤來驗證存取

## 安全追蹤的運作方式

您可以新增權限追蹤篩選器、以指示ONTAP Sfin記錄儲存虛擬機器（SVM）上SMB和NFS伺服器為何允許或拒絕用戶端或使用者執行作業的要求。當您想要驗證檔案存取安全性配置是否適當、或是想要疑難排解檔案存取問題時、這項功能就很實用。

安全追蹤可讓您設定篩選器、偵測SVM上SMB和NFS上的用戶端作業、並追蹤符合該篩選器的所有存取檢查。然後您可以檢視追蹤結果、以方便的方式摘要說明允許或拒絕存取的原因。

當您想要驗證SVM上檔案和資料夾的SMB或NFS存取安全性設定、或是遇到存取問題時、可以快速新增篩選器來開啟權限追蹤。

下列清單概述安全追蹤運作方式的重要事實：

- 在SVM層級套用安全追蹤。ONTAP
- 每個傳入要求都會經過篩選、以查看是否符合任何已啟用安全追蹤的篩選條件。
- 檔案和資料夾存取要求都會執行追蹤。
- 追蹤可以根據下列準則進行篩選：
  - 用戶端 IP
  - SMB或NFS路徑
  - Windows名稱
  - UNIX 名稱
- 系統會針對「允許」和「拒絕」存取回應結果進行篩選。
- 每個符合已啟用追蹤篩選條件的要求、都會記錄在追蹤結果記錄中。
- 儲存管理員可在篩選器上設定逾時、以自動停用篩選器。
- 如果某個要求符合多個篩選器、則會記錄索引編號最高的篩選器結果。
- 儲存管理員可從追蹤結果記錄列印結果、以判斷允許或拒絕存取要求的原因。

## 存取類型會檢查監控的安全追蹤

檔案或資料夾的存取檢查是根據多個準則進行。安全追蹤會監控所有這些準則的作業。

安全追蹤監控的存取檢查類型包括：

- Volume與qtree安全樣式
- 檔案系統的有效安全性、其中包含要求執行作業的檔案和資料夾
- 使用者對應
- 共用層級權限

- 匯出層級權限
- 檔案層級權限
- 儲存層級的存取保護安全性

## 建立安全追蹤時的考量

在儲存虛擬機器（SVM）上建立安全追蹤時、請謹記幾個考量事項。例如、您需要知道可以建立追蹤的通訊協定、支援哪些安全性樣式、以及最大作用中追蹤數量。

- 您只能在SVM上建立安全追蹤。
- 每個安全性追蹤篩選器項目都是SVM專屬項目。

您必須指定要在其中執行追蹤的SVM。

- 您可以新增SMB和NFS要求的權限追蹤篩選器。
- 您必須在要建立追蹤篩選器的SVM上設定SMB或NFS伺服器。
- 您可以為位於NTFS、UNIX及混合式安全型磁碟區和qtree上的檔案和資料夾建立安全追蹤。
- 每個SVM最多可新增10個權限追蹤篩選器。
- 建立或修改篩選時、必須指定篩選索引編號。

篩選條件會依索引編號的順序進行考量。索引編號較高的篩選條件、會在索引編號較低的條件之前考量。如果要追蹤的要求符合多個已啟用篩選器中的條件、則只會觸發索引編號最高的篩選器。

- 建立並啟用安全性追蹤篩選器之後、您必須在用戶端系統上執行部分檔案或資料夾要求、以產生追蹤篩選器可擷取並登入追蹤結果記錄的活動。
- 您應該新增權限追蹤篩選器、僅供檔案存取驗證或疑難排解之用。

新增權限追蹤篩選器對控制器效能的影響不大。

完成驗證或疑難排解活動後、您應該停用或移除所有權限追蹤篩選器。此外、您選取的篩選條件應盡可能明確、ONTAP 以便不將大量的追蹤結果傳送到記錄檔。

## 執行安全追蹤

### 執行安全追蹤總覽

執行安全性追蹤包括建立安全性追蹤篩選器、驗證篩選條件、在符合篩選條件的SMB或NFS用戶端上產生存取要求、以及檢視結果。

完成使用安全篩選器擷取追蹤資訊之後、您可以修改篩選器並重複使用、或是在不再需要時停用篩選器。檢視及分析篩選追蹤結果之後、您可以在不再需要時將其刪除。

## 建立安全追蹤篩選器

您可以建立安全追蹤篩選器、以偵測儲存虛擬機器（SVM）上的SMB和NFS用戶端作業、並追蹤符合篩選器的所有存取檢查。您可以使用安全追蹤的結果來驗證組態或疑難排解存取問題。

關於這項工作

Vserver安全追蹤篩選器create命令需要兩個參數：

| 必要參數                                | 說明   |
|-------------------------------------|--|
| <code>-vserver vservice_name</code> | <b>SVM名稱</b><br><br>包含您要套用安全性追蹤篩選器之檔案或資料夾的SVM名稱。                 |
| <code>-index index_number</code>    | <b>篩選索引編號</b><br><br>要套用至篩選的索引編號。每個SVM最多可有10個追蹤篩選器。此參數允許的值為1到10。 |

許多選用的篩選參數可讓您自訂安全性追蹤篩選器、以便縮小安全性追蹤所產生的結果：

| 篩選參數  | 說明  |
|---|---|
| <code>-client-ip IP_Address</code>  | 此篩選器會指定使用者存取SVM的IP位址。   |
| <code>-path path</code>   | 此篩選器會指定要套用權限追蹤篩選器的路徑。的價值 <code>-path</code> 可以使用下列其中一種格式： <ul style="list-style-type: none"><li>• 完整路徑、從共用區根目錄或匯出開始</li><li>• 部分路徑、相對於共用的根目錄</li></ul> 您必須在路徑值中使用NFS樣式目錄UNIX型目錄分隔符號。  |
| <code>-windows-name win_user_name</code><br>或 <code>-unix</code><br><code>-name`unix_user_name</code> | 您可以指定要追蹤其存取要求的Windows使用者名稱或UNIX使用者名稱。使用者名稱變數不區分大小寫。您無法在同一個篩選器中同時指定Windows使用者名稱和UNIX使用者名稱。 <div> 即使您可以追蹤SMB和NFS存取事件、對應的UNIX使用者和對應的UNIX使用者群組也可以在混合或UNIX安全型資料上執行存取檢查。</div> |
| <code>-trace-allow {yes</code>  | <code>no}</code>  |

|   |                                     |
|---|-------------------------------------|
| 安全性追蹤篩選器一律會啟用拒絕事件追蹤。您可以選擇追蹤允許事件。若要追蹤允許事件、請將此參數設為 yes。 | -enabled {enabled                   |
| disabled}   | 您可以啟用或停用安全性追蹤篩選器。依預設、安全性追蹤篩選器為啟用狀態。 |
| -time-enabled integer                                 | 您可以指定篩選器的逾時時間、之後篩選器就會停用。            |

## 步驟

### 1. 建立安全追蹤篩選器：

```
vserver security trace filter create -vserver vserver_name -index
index_number filter_parameters
```

filter\_parameters 為選用篩選參數清單。

如需詳細資訊、請參閱命令的手冊頁。

### 2. 驗證安全性追蹤篩選器項目：

```
vserver security trace filter show -vserver vserver_name -index index_number
```

## 範例

下列命令會為任何使用者建立安全性追蹤篩選器、以存取具有共用路徑的檔案

\\server\share1\dir1\dir2\file.txt 從 IP 位址 10.10.10.7。篩選器使用的完整路徑 -path 選項。用於存取資料的用戶端 IP 位址為 10.10.10.7。篩選器在 30 分鐘後逾時：

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver   Index   Client-IP           Path                Trace-Allow
Windows-Name
-----
vs1        1       10.10.10.7         /dir1/dir2/file.txt          no          -
```

下列命令會使用的相對路徑來建立安全性追蹤篩選器 -path 選項。篩選器會追蹤名為「joe」之 Windows 使用者的存取權。Joe 正在存取具有共用路徑的檔案 \\server\share1\dir1\dir2\file.txt。篩選器追蹤會允許及拒絕事件：

```
cluster1::> vservers security trace filter create -vservers vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vservers security trace filter show -vservers vs1 -index 2
Vserver: vs1
Filter Index: 2
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: mydomain\joe
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

## 顯示安全追蹤篩選器的相關資訊

您可以顯示儲存虛擬機器（SVM）上設定的安全追蹤篩選器相關資訊。這可讓您查看每個篩選器追蹤的存取事件類型。

### 步驟

1. 使用顯示安全性追蹤篩選項目的相關資訊 `vservers security trace filter show` 命令。

如需使用此命令的詳細資訊、請參閱手冊頁。

### 範例

下列命令會顯示SVM VS1上所有安全追蹤篩選器的相關資訊：

```
cluster1::> vservers security trace filter show -vservers vs1
Vserver  Index  Client-IP          Path                Trace-Allow
Windows-Name
-----  -
vs1      1      -                  /dir1/dir2/file.txt  yes
vs1      2      -                  /dir3/dir4/          no
mydomain\joe
```

## 顯示安全性追蹤結果

您可以顯示針對符合安全性追蹤篩選器的檔案作業所產生的安全性追蹤結果。您可以使用結果來驗證檔案存取安全性組態、或疑難排解SMB和NFS檔案存取問題。

### 您需要的產品

啟用的安全性追蹤篩選器必須存在、而且必須從SMB或NFS用戶端執行作業、且該用戶端必須符合安全性追蹤

篩選器、才能產生安全性追蹤結果。

#### 關於這項工作

您可以顯示所有安全性追蹤結果的摘要、也可以指定選用參數來自訂輸出中顯示的資訊。當安全性追蹤結果包含大量記錄時、這一點很有幫助。

如果您未指定任何選用參數、則會顯示下列項目：

- 儲存虛擬機器（SVM）名稱
- 節點名稱
- 安全性追蹤索引編號
- 安全風格
- 路徑
- 理由
- 使用者名稱

使用者名稱會根據追蹤篩選器的設定方式顯示：

| 如果篩選器已設定...    | 然後...                   |
|----------------|-------------------------|
| 使用UNIX使用者名稱    | 安全性追蹤結果會顯示UNIX使用者名稱。    |
| 使用Windows使用者名稱 | 安全性追蹤結果會顯示Windows使用者名稱。 |
| 沒有使用者名稱        | 安全性追蹤結果會顯示Windows使用者名稱。 |

您可以使用選用參數來自訂輸出。您可以使用某些選用參數來縮小命令輸出中傳回的結果範圍、其中包括：

| 選用參數                                  | 說明  |
|---------------------------------------|---|
| <code>-fields field_name \ ...</code> | 在您選擇的欄位上顯示輸出。您可以單獨使用此參數、也可以搭配其他選用參數一起使用。      |
| <code>-instance</code>                | 顯示安全性追蹤事件的詳細資訊。此參數可搭配其他選用參數使用、以顯示特定篩選結果的詳細資訊。 |
| <code>-node node_name</code>          | 僅顯示有關指定節點上事件的資訊。                              |
| <code>-vserver vsver_name</code>      | 僅顯示指定SVM上事件的相關資訊。                             |
| <code>-index integer</code>           | 顯示與指定索引編號對應之篩選器所產生之事件的相關資訊。                   |
| <code>-client-ip IP_address</code>    | 顯示從指定用戶端IP位址存取檔案所發生事件的相關資訊。                   |



|   |                                     |
|---|-------------------------------------|
| <code>-path path</code>                     | 顯示因檔案存取指定路徑而發生事件的相關資訊。              |
| <code>-user-name user_name</code>           | 顯示指定Windows或UNIX使用者存取檔案時所發生事件的相關資訊。 |
| <code>-security-style security_style</code> | 顯示在具有指定安全樣式的檔案系統上發生事件的相關資訊。         |

請參閱手冊頁、以取得可搭配命令使用的其他選用參數資訊。

## 步驟

1. 使用顯示安全性追蹤篩選結果 `vserver security trace trace-result show` 命令。

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1
```

| Node  | Index | Filter Details   | Reason                        |
|-------|-------|--|-------------------------------|
| ----- | ----- | -----  | -----                         |
| node1 | 3     | User:domain\user<br>Security Style:mixed<br>Path:/dir1/dir2/ | Access denied by explicit ACE |
| node1 | 5     | User:domain\user<br>Security Style:unix<br>Path:/dir1/       | Access denied by explicit ACE |

## 修改安全性追蹤篩選器

如果您想要變更選用的篩選參數、以決定追蹤哪些存取事件、您可以修改現有的安全性追蹤篩選器。

### 關於這項工作

您必須指定要套用篩選器的儲存虛擬機器 (SVM) 名稱、以及篩選器的索引編號、以識別要修改的安全性追蹤篩選器。您可以修改所有選用的篩選參數。

## 步驟

1. 修改安全性追蹤篩選器：

```
vserver security trace filter modify -vserver vserver_name -index  
index_numberfilter_parameters
```

- `vserver_name` 是要套用安全性追蹤篩選器的 SVM 名稱。
- `index_number` 是您要套用至篩選的索引編號。此參數允許的值為1到10。

◦ `filter_parameters` 為選用篩選參數清單。

## 2. 驗證安全性追蹤篩選器項目：

```
vserver security trace filter show -vserver vserver_name -index index_number
```

### 範例

下列命令會修改索引編號為1的安全性追蹤篩選器。篩選器會追蹤任何使用者存取具有共用路徑之檔案的事件 `\\server\share1\dir1\dir2\file.txt` 來自任何 IP 位址。篩選器使用的完整路徑 `-path` 選項。篩選器追蹤會允許及拒絕事件：

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
          Vserver: vs1
          Filter Index: 1
Client IP Address to Match: -
          Path: /dir1/dir2/file.txt
Windows User Name: -
UNIX User Name: -
Trace Allow Events: yes
          Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

## 刪除安全追蹤篩選器

當您不再需要安全性追蹤篩選器項目時、可以將其刪除。由於每個儲存虛擬機器（SVM）最多可有10個安全追蹤篩選器、因此刪除不需要的篩選器後、您就能在達到上限時建立新的篩選器。

### 關於這項工作

若要唯一識別您要刪除的安全性追蹤篩選器、您必須指定下列項目：

- 套用追蹤篩選器的SVM名稱
- 追蹤篩選器的篩選索引編號

### 步驟

#### 1. 識別您要刪除之安全性追蹤篩選器項目的篩選器索引編號：

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path                | Trace-Allow | Windows-Name |
|--------------|-------|-----------|---------------------|-------------|--------------|
| -----        | ----- | -----     | -----               | -----       | -----        |
| vs1          | 1     | -         | /dir1/dir2/file.txt | yes         | -            |
| vs1          | 2     | -         | /dir3/dir4/         | no          |              |
| mydomain\joe |       |           |                     |             |              |

## 2. 使用上一個步驟的篩選索引編號資訊、刪除篩選項目：

```
vserver security trace filter delete -vserver vs1 -index 1
```

```
vserver security trace filter delete -vserver vs1 -index 1
```

## 3. 確認安全性追蹤篩選器項目已刪除：

```
vserver security trace filter show -vserver vs1
```

```
vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path        | Trace-Allow | Windows-Name |
|--------------|-------|-----------|-------------|-------------|--------------|
| -----        | ----- | -----     | -----       | -----       | -----        |
| vs1          | 2     | -         | /dir3/dir4/ | no          |              |
| mydomain\joe |       |           |             |             |              |

## 刪除安全性追蹤記錄

使用篩選器追蹤記錄來驗證檔案存取安全性或疑難排解SMB或NFS用戶端存取問題之後、您可以從安全性追蹤記錄中刪除安全性追蹤記錄。

關於這項工作

在刪除安全性追蹤記錄之前、您必須知道記錄的序號。



每個儲存虛擬機器（SVM）最多可儲存128筆追蹤記錄。如果SVM達到上限、則會在新增追蹤記錄時自動刪除最舊的追蹤記錄。如果您不想手動刪除此SVM上的追蹤記錄、ONTAP 可讓SVM在達到最大值後自動刪除最舊的追蹤結果、以便留出新結果的空間。

## 步驟

### 1. 識別您要刪除的記錄序號：

```
vserver security trace trace-result show -vserver vs1 -instance
```

### 2. 刪除安全性追蹤記錄：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer
```

```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

◦ `-node node_name` 是您要刪除之權限追蹤事件所在的叢集節點名稱。

這是必要的參數。

◦ `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的 SVM 名稱。

這是必要的參數。

◦ `-seqnum integer` 為您要刪除的記錄事件序號。

這是必要的參數。

## 刪除所有安全追蹤記錄

如果您不想保留任何現有的安全性追蹤記錄、可以使用單一命令刪除節點上的所有記錄。

### 步驟

1. 刪除所有安全追蹤記錄：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

◦ `-node node_name` 是您要刪除之權限追蹤事件所在的叢集節點名稱。

◦ `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的儲存虛擬機器（SVM）名稱。

## 解讀安全性追蹤結果

安全性追蹤結果提供允許或拒絕要求的原因。輸出會結合允許或拒絕存取的原因、以及允許或拒絕存取的存取檢查路徑中的位置、來顯示結果。您可以使用結果來隔離及識別為何允許或不允許採取行動。

### 尋找結果類型清單和篩選詳細資料的相關資訊

您可以在的手冊頁中找到可包含在安全追蹤結果中的結果類型清單和篩選詳細資料 `vserver security trace trace-result show` 命令。

的輸出範例 Reason 欄位 Allow 結果類型

以下是的輸出範例 Reason 出現在追蹤結果中的欄位會登入 Allow 結果類型：

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

的輸出範例 Reason 欄位 Allow 結果類型

以下是的輸出範例 Reason 出現在追蹤結果中的欄位會登入 Deny 結果類型：

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

的輸出範例 Filter details 欄位

以下是的輸出範例 Filter details 追蹤結果記錄中的欄位、其中列出檔案系統的有效安全樣式、其中包含符合篩選條件的檔案和資料夾：

```
Security Style: MIXED and ACL
```

## 何處可找到其他資訊

成功測試 SMB 用戶端存取之後、您可以執行進階 SMB 組態或新增 SAN 存取。成功測試 NFS 用戶端存取之後、您可以執行進階 NFS 組態或新增 SAN 存取。傳輸協定存取完成時、您應該保護 SVM 的根 Volume。

### SMB 組態

您可以使用下列項目來進一步設定 SMB 存取：

- ["中小企業管理"](#)

說明如何使用 SMB 通訊協定來設定及管理檔案存取。

- ["NetApp 技術報告 4191：叢集 Data ONTAP 式更新的最佳實務做法指南 8.2 Windows 檔案服務"](#)

提供 SMB 實作與其他 Windows 檔案服務功能的簡短概述、並提供 ONTAP 有關的建議與基本疑難排解資訊。

- ["NetApp 技術報告 3740：SMB 2 Next-Generation CIFS Protocol in Data ONTAP"](#)

介紹 SMB 2 的功能、組態詳細資料、以及 ONTAP 其在功能方面的實作。

## NFS 組態

您可以使用下列項目進一步設定NFS存取：

- ["NFS管理"](#)

說明如何使用NFS傳輸協定來設定及管理檔案存取。

- ["NetApp技術報告4067：NFS最佳實務與實作指南"](#)

可做為NFSv3和NFSv3作業指南、提供ONTAP 關於以NFSv3為焦點的各種作業系統的概述。

- ["NetApp技術報告4668：名稱服務最佳實務做法指南"](#)

提供完整的最佳實務做法、限制、建議及考量清單、以供設定LDAP、NIS、DNS及本機使用者與群組檔案進行驗證。

- ["NetApp技術報告4616：ONTAP NFS Kerberos in Some with Microsoft Active Directory"](#)

- ["NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"](#)

- ["NetApp技術報告3580：NFSv4增強功能與最佳實務做法指南Data ONTAP -實作"](#)

說明在掛接到執行ONTAP 此功能的系統上、在AIX、Linux或Solaris用戶端上實作NFSv4元件時應遵循的最佳實務做法。

## 根Volume保護

在SVM上設定傳輸協定之後、您應確保其根Volume受到保護：

- ["資料保護"](#)

說明如何建立負載共用鏡像來保護SVM根磁碟區、這是NetApp啟用NAS的SVM最佳實務做法。同時也說明如何從負載共用鏡像中提升SVM根磁碟區、以快速從磁碟區故障或損失中恢復。

## 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。