



# 可稽核的**CLI**變更事件

## ONTAP 9

NetApp  
February 12, 2026

# 目錄

可稽核的CLI變更事件 .....	1
瞭解可稽核的 ONTAP CLI 變更事件 .....	1
管理檔案共用 ONTAP 事件 .....	2
管理稽核原則變更 ONTAP 事件 .....	3
管理使用者帳戶 ONTAP 事件 .....	4
管理安全性群組 ONTAP 事件 .....	5
管理授權原則變更 ONTAP 事件 .....	6

# 可稽核的CLI變更事件

## 瞭解可稽核的 ONTAP CLI 變更事件

可稽核某些CLI變更事件、包括特定SMB共用事件、特定稽核原則事件、特定本機安全性群組事件、本機使用者群組事件、以及授權原則事件。ONTAP瞭解哪些變更事件可稽核、有助於解讀事件記錄的結果。

您可以手動旋轉稽核記錄、啟用或停用稽核、顯示稽核變更事件的相關資訊、修改稽核變更事件、以及刪除稽核變更事件、藉此管理儲存虛擬機器 (SVM) 稽核CLI變更事件。

身為系統管理員、如果您執行任何命令來變更SMB共用區、本機使用者群組、本機安全性群組、授權原則及稽核原則事件的相關組態、產生記錄並稽核相應的事件：

稽核類別	活動	事件ID	執行此命令...
主機稽核	原則變更	[4719]稽核組態已變更	<code>`vserver audit disable</code>
enable	<code>modify`</code>	檔案共用	已新增[5142]網路共用
<code>vserver cifs share create</code>	[5143]網路共用區已修改	<code>vserver cifs share modify `vserver cifs share create</code>	<code>modify</code>
<code>delete` `vserver cifs share add</code>	<code>remove`</code>	[5144]網路共用區已刪除	<code>vserver cifs share delete</code>
稽核	使用者帳戶	[4720]本機使用者已建立	<code>vserver cifs users-and-groups local-user create vserver services name-service unix-user create</code>
[4722]本機使用者已啟用	<code>`vserver cifs users-and-groups local-user create</code>	<code>modify`</code>	[4724]本機使用者密碼重設
<code>vserver cifs users-and-groups local-user set-password</code>	[4725]本機使用者已停用	<code>`vserver cifs users-and-groups local-user create</code>	<code>modify`</code>

[4726]本機使用者已刪除	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738]本機使用者變更	vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify
[4781]本機使用者重新命名	vserver cifs users-and-groups local-user rename	安全性群組	[4731]已建立本機安全性群組
vserver cifs users-and-groups local-group create vserver services name-service unix-group create	[4734]本機安全性群組已刪除	vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete	[4735]本機安全性群組已修改
`vserver cifs users-and-groups local-group rename	modify` vserver services name-service unix-group modify	[4732]使用者已新增至本機群組	vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser
[4733]使用者已從本機群組中移除	vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser	授權原則變更	[4704]已指派使用者權限
vserver cifs users-and-groups privilege add-privilege	[4705]使用者權限已移除	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

#### 相關資訊

- ["Vserver"](#)

## 管理檔案共用 ONTAP 事件

為儲存虛擬機器（SVM）設定檔案共用事件並啟用稽核時、就會產生稽核事件。使用修改 SMB 網路共用時、會產生檔案共用事件 `vserver cifs share` 相關命令。

新增、修改或刪除SVM的SMB網路共用時、會產生事件ID為5142、5143和5144的檔案共用事件。SMB 網路共

用組態是使用修改的 `cifs share access control create|modify|delete` 命令。

下列範例顯示建立名為「稽核目的地」的共用物件時、會產生ID為5143的檔案共用事件：

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name] NetApp-Security-Auditing
    [ Guid] {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID 5142
    EventName Share Object Added
    ...
    ...
    ShareName audit_dest
    SharePath /audit_dest
    ShareProperties oplocks;browsable;changenotify;show-previous-versions;
    SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

## 管理稽核原則變更 ONTAP 事件

當為儲存虛擬機器（SVM）設定稽核原則變更事件並啟用稽核時、就會產生稽核事件。使用修改稽核原則時、會產生稽核原則變更事件 `vserver audit` 相關命令。

每當停用、啟用或修改稽核原則時、就會產生事件ID 4719的稽核原則變更事件、並有助於識別使用者嘗試停用稽核以涵蓋追蹤的時間。此設定預設為設定、需要診斷權限才能停用。

下列範例顯示稽核原則變更事件、並在停用稽核時產生ID 4719：

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
    [ Name] NetApp-Security-Auditing
    [ Guid] {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID 4719
    EventName Audit Disabled
    ...
    ...
    SubjectUserName admin
    SubjectUserSid 65533-1001
    SubjectDomainName ~
    SubjectIP console
    SubjectPort
```

## 管理使用者帳戶 ONTAP 事件

當儲存虛擬機器 (SVM) 的使用者帳戶事件設定為啟用稽核時、就會產生稽核事件。

事件ID為4720、4722、4724、4725、4726、當本機SMB或NFS使用者從系統建立或刪除、本機使用者帳戶啟用、停用或修改、以及本機SMB使用者密碼重設或變更時、就會產生4738和4781。使用修改使用者帳戶時、會產生使用者帳戶事件 `vserver cifs users-and-groups <local user>` 和 `vserver services name-service <unix user>` 命令。

下列範例顯示建立本機SMB使用者時產生ID 4720的使用者帳戶事件：

```
netapp-clus1::~* > vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
- Provider
  [ Name] NetApp-Security-Auditing
  [ Guid] {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
EventID 4720
EventName Local Cifs User Created
...
...
TargetUserName testuser
TargetDomainName NETAPP-CLUS1
TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
TargetType CIFS
DisplayName testuser
PasswordLastSet 1472662216
AccountExpires NO
PrimaryGroupId 513
UserAccountControl %%0200
SidHistory ~
PrivilegeList ~
```

下列範例顯示在先前範例中建立的本機SMB使用者重新命名時、產生ID為4781的使用者帳戶事件：

```
netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

## 管理安全性群組 ONTAP 事件

當儲存虛擬機器 (SVM) 的安全性群組事件設定為啟用稽核時、就會產生稽核事件。

從系統建立或刪除本機SMB或NFS群組、並從群組新增或移除本機使用者時、會產生事件ID為4731、4732、4733、4734和4735的安全性群組事件。當使用修改使用者帳戶時、就會產生安全性群組事件 `vserver cifs users-and-groups <local-group>` 和 `vserver services name-service <unix-group>` 命令。

下列範例顯示建立本機UNIX安全性群組時、產生ID 4731的安全性群組事件：

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

## 管理授權原則變更 ONTAP 事件

當儲存虛擬機器 (SVM) 的授權原則變更事件設定為啟用稽核時、就會產生稽核事件。

每當SMB使用者和SMB群組的授權權限被授予或撤銷時、就會產生事件ID為4704和4705的授權原則變更事件。當使用指派或撤銷授權權限時、就會產生授權原則變更事件 `vserver cifs users-and-groups privilege` 相關命令。

下列範例顯示指派SMB使用者群組授權權限時、產生ID 4704的授權原則事件：

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name] NetApp-Security-Auditing
  [ Guid] {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID 4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

## 版權資訊

Copyright © 2026 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。