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

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	`vserver audit disable
enable	modify`	檔案共用	已新增[5142]網路共用
`vserver cifs share create`	[5143]網路共用區已修改	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144]網路共用區已刪除	`vserver cifs share delete`
稽核	使用者帳戶	[4720]本機使用者已建立	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722]本機使用者已啟用	`vserver cifs users-and-groups local-user create	modify`	[4724]本機使用者密碼重設
`vserver cifs users-and-groups local-user set-password`	[4725]本機使用者已停用	`vserver cifs users-and-groups local-user create	modify`

[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
```