監査できる**CLI**変更イベント

ONTAP 9

NetApp
February 12, 2026

目次

監査できるCLI変更イベント

監査可能なONTAP CLIの変更イベントについて学習します

ONTAPでは、SMB共有イベント、監査ポリシー イベント、ローカル セキュリティ グループ イベント、ローカル ユーザ グループ イベント、認証ポリシー イベントなどのCLI変更イベントを監査できます。どのような変更イベントを監査できるか理解しておくと、イベント ログの結果を解釈するときに役立ちます。

Storage Virtual Machine（SVM）で監査するCLI変更イベントの管理作業として、手動での監査ログのローテーション、監査の有効化と無効化、監査対象変更イベントに関する情報の表示、監査対象変更イベントの変更、監査対象変更イベントの削除が可能です。

管理者がSMB共有、ローカル ユーザ グループ、ローカル セキュリティ グループ、認証ポリシー、および監査ポリシーのイベントに関連する設定を変更するコマンドを実行すると、レコードが生成され、対応するイベントが監査されます。

監査カテゴリ	イベント	イベント ID	このコマンドを実行します…
Mhostの監査	policy-change	[4719] 監査設定が変更されました	`vserver audit disable
enable	modify`	ファイル共有	[5142] ネットワーク共有が追加されました
`vserver cifs share create`	[5143] ネットワーク共有が変更されました	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] ネットワーク共有が削除されました	`vserver cifs share delete`
監査	ユーザーアカウント	[4720] ローカルユーザーが作成されました	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] ローカルユーザーが有効	`vserver cifs users-and-groups local-user create	modify`	[4724] ローカルユーザーのパスワードリセット
`vserver cifs users-and-groups local-user set-password`	[4725] ローカルユーザーが無効になっています	`vserver cifs users-and-groups local-user create	modify`

[4726] ローカルユーザーが削除されました	`vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete`	[4738] ローカルユーザーの変更	`vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify`
[4781] ローカルユーザーの名前変更	`vserver cifs users-and-groups local-user rename`	セキュリティグループ	[4731] ローカルセキュリティグループが作成されました
`vserver cifs users-and-groups local-group create vserver services name-service unix-group create`	[4734] ローカルセキュリティグループが削除されました	`vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete`	[4735] ローカルセキュリティグループが変更されました
`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] ユーザーがローカルグループに追加されました	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] ユーザーがローカル グループから削除されました	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	承認ポリシーの変更	[4704] ユーザー権限が割り当てられました
`vserver cifs users-and-groups privilege add-privilege`	[4705] ユーザー権限が削除されました	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`	

関連情報

- "SVM"

ファイル共有ONTAPイベントを管理する

ストレージ仮想マシン（SVM）にファイル共有イベントが設定され、監査が有効になっている場合、監査イベントが生成されます。ファイル共有イベントは、`vserver cifs share`関連コマンドを使用してSMBネットワーク共有が変更されたときに生成されます。

イベントID 5142、5143、5144 のファイル共有イベントは、SVM の SMB ネットワーク共有が追加、変更、または削除されたときに生成されます。SMB ネットワーク共有の設定は、 `cifs share access control create|modify|delete`コマンドを使用して変更されます。

次の例では、「audit_dest」という名前の共有オブジェクトが作成され、ID 5143のfile-shareイベントが生成されています。

```
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)
```

監査ポリシー変更の**ONTAP**イベントを管理する

ストレージ仮想マシン（SVM）に監査ポリシー変更イベントが設定され、監査が有効になっている場合、監査イベントが生成されます。監査ポリシー変更イベントは、 `vserver audit`関連コマンドを使用して監査ポリシーが変更されたときに生成されます。

イベントID 4719の監査ポリシー変更イベントは、監査ポリシーが無効化、有効化、または変更されるたびに生成され、ユーザーが痕跡を隠蔽するために監査を無効化しようとしたタイミングを特定するのに役立ちます。このイベントはデフォルトで設定されており、無効化には診断権限が必要です。

次の例では、監査が無効にされたときにID 4719のaudit-policy-changeイベントが生成されています。

```
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
```

ユーザーアカウントの**ONTAP**イベントを管理する

Storage Virtual Machine（SVM）に対してuser-accountイベントが設定されていて、監査が有効になっている場合、監査イベントが生成されます。

イベントID 4720、4722、4724、4725、4726、4738、および 4781 のユーザーアカウントイベントは、ローカル SMB または NFS ユーザーがシステムから作成または削除された場合、ローカルユーザーアカウントが有効化、無効化、または変更された場合、およびローカル SMB ユーザーのパスワードがリセットまたは変更された場合に生成されます。ユーザーアカウントイベントは、 `vserver cifs users-and-groups <*local user*>`および `vserver services name-service <*unix user*>`コマンドを使用してユーザーアカウントが変更された場合に生成されます。

次の例は、ローカル SMB ユーザーが作成されたときに生成された ID 4720 のユーザー アカウント イベントを示しています：

```
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 ~
```

次の例は、前の例で作成されたローカルSMBユーザーの名前が変更されたときに生成される、ID 4781のユーザー アカウント イベントを示しています：

```
 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 ~
```

セキュリティグループの**ONTAP**イベントを管理する

Storage Virtual Machine（SVM）に対してsecurity-groupイベントが設定されていて、監査が有効になっている場合、監査イベントが生成されます。

イベント ID 4731、4732、4733、4734、4735 のセキュリティグループイベントは、ローカル SMB または NFS グループがシステムから作成または削除されたとき、およびローカルユーザーがグループに追加または削除されたときに生成されます。セキュリティグループイベントは、 `vserver cifs users-and-groups <*local-group*>`コマンドおよび `vserver services name-service <*unix-group*>`コマンドを使用してユーザーアカウントが変更されたときに生成されます。

次の例では、ローカルUNIXセキュリティ グループが作成され、ID 4731のsecurity-groupイベントが生成されています。

```
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 ~
```

認可ポリシー変更のONTAPイベントを管理する

Storage Virtual Machine（SVM）に対してauthorization-policy-changeイベントが設定されていて、監査が有効になっている場合、監査イベントが生成されます。

イベントID 4704 および 4705 の authorization-policy-change イベントは、SMB ユーザーおよび SMB グループに対して認可権限が付与または取り消されるたびに生成されます。authorization-policy-change イベントは、 `vserver cifs users-and-groups privilege`関連コマンドを使用して認可権限が割り当てまたは取り消された場合に生成されます。

次の例では、SMBユーザ グループに対する認証権限が割り当てられ、ID 4704の認証ポリシー イベントが生成されています。

```
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
```

著作権に関する情報

商標に関する情報