



# 監査できるCLI変更イベント ONTAP 9

NetApp  
December 20, 2024

# 目次

監査できるCLI変更イベント .....	1
監査できるCLI変更イベントの概要 .....	1
ファイルキヨウユウイヘントノカンリ .....	2
カンサホリシイヘンコウイヘントノカンリ .....	3
ユーザアカウントイベントの管理 .....	4
セキュリティグループイベントの管理 .....	6
認証ポリシー変更イベントの管理 .....	7

# 監査できるCLI変更イベント

## 監査できるCLI変更イベントの概要

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、特定のCLI変更イベントを監査できます。どの変更イベントを監査できるかを理解しておく、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) によるCLI変更イベントの監査の管理作業として、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、監査変更イベントに関する情報の表示、監査変更イベントの変更、監査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各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 IDs	実行するコマンド
Mhostの監査	ポリシー変更	[4719] 監査設定が変更されました	<code>`vserver audit disable</code>
enable	<code>modify`</code>	ファイル共有	[5142] ネットワーク共有が追加されました
<code>vserver cifs share create</code>	[5143] ネットワーク共有の変更	<code>vserver cifs share modify `vserver cifs share create</code>	<code>modify</code>
<code>delete` `vserver cifs share add</code>	<code>remove`</code>	[5144] ネットワーク共有が削除されました	<code>vserver cifs share delete</code>
監査	ユーザアカウント	[4720] ローカルユーザの作成	<code>vserver cifs users-and-groups local-user create vserver services name-service unix-user create</code>
[4722] ローカルユーザの有効化	<code>`vserver cifs users-and-groups local-user create</code>	<code>modify`</code>	[4724] ローカルユーザのパスワードのリセット
<code>vserver cifs users-and-groups local-user set-password</code>	[4725] ローカルユーザの無効化	<code>`vserver cifs users-and-groups local-user create</code>	<code>modify`</code>

[4726] ローカルユーザの削除	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738] ローカルユーザの変更	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の変更
`vserver cifs users-and-groups local-group rename	modify` vserver services name-service unix-group modify	[4732] ローカルグループへのユーザの追加	vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser
[4733] ローカルグループからユーザが削除されました	vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser	認証ポリシー変更	[4704] ユーザ権限の割り当て
vserver cifs users-and-groups privilege add-privilege	[4705] ユーザ権限が削除されました	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

## ファイルキヨウユウイヘントノカンリ

Storage Virtual Machine (SVM) に対してファイル共有イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。ファイル共有イベントが生成されるのは、の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場合 `vserver cifs share` です。

ファイル共有イベントは、SVMに対して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。イベントIDは5142、5143、および5144です。SMBネットワーク共有の設定は、コマンドを使用し

て変更し `cifs share access control create|modify|delete` 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が5143のファイル共有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)
```

## カンサホリシイヘンコウイヘントノカンリ

Storage Virtual Machine (SVM) に対して監査ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての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、の関連コマンドを使用して監査ポリシーが変更された場合に生成され `vserver audit` ます。

監査ポリシー変更イベント（イベントID 4719）は、監査ポリシーが無効、有効、または変更されたときに生成され、ユーザが監査を無効にしようとしたタイミングを特定して追跡できます。このイベントはデフォルトで設定されており、無効にするには diagnostic 権限が必要です。

次の例では、監査が無効になっているときに、ID 4719の監査ポリシー変更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
```

## ユーザアカウントイベントの管理

Storage Virtual Machine (SVM) に対してユーザアカウントイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

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

次の例では、ローカルSMBユーザが作成され、ID 4720のユーザアカウントイベントが生成されています。

```
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 ~
```

次の例では、上記の例で作成されたローカルSMBユーザの名前が変更され、ID 4781のユーザアカウントイベントが生成されています。

```
netapp-clus1::*> vsserver 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イベントの管理

Storage Virtual Machine (SVM) に対してセキュリティグループイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

セキュリティグループイベントは、システムのローカル SMB グループまたは NFS グループが作成または削除されたとき、それらのグループのローカルユーザが追加または削除されたときに生成されます。イベント ID は 4731、4732、4733、4734、および 4735 です。セキュリティグループイベントは、コマンドおよび `vsserver services name-service <unix-group>` コマンドを使用してユーザアカウントが変更されたときに生成され `vsserver cifs users-and-groups <local-group>` 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のセキュリティグループ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 ~
```

## 認証ポリシー変更イベントの管理

Storage Virtual Machine (SVM) に対して認証ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

認証ポリシー変更イベントは、SMBユーザおよびSMBグループに対して認証権限が付与または取り消されるたびに生成されます。イベントIDは4704および4705です。認証ポリシー変更イベントが生成されるのは、の関連コマンドを使用して認証権限が割り当てられた場合または取り消された場合 `vserver cifs users-and-groups privilege` です。

次の例では、SMBユーザグループの認証権限が割り当てられている場合に、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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。