



감사할 수 있는 **CLI** 변경 이벤트입니다 ONTAP 9

NetApp
February 12, 2026

목차

감사할 수 있는 CLI 변경 이벤트입니다	1
감사 가능한 ONTAP CLI 변경 이벤트에 대해 알아보십시오	1
파일 공유 ONTAP 이벤트를 관리합니다	2
감사 정책 변경 ONTAP 이벤트를 관리합니다	3
사용자 계정 ONTAP 이벤트를 관리합니다	4
보안 그룹 ONTAP 이벤트를 관리합니다	5
authorization-policy-change ONTAP 이벤트를 관리합니다	6

감사할 수 있는 CLI 변경 이벤트입니다

감사 가능한 ONTAP CLI 변경 이벤트에 대해 알아보십시오

ONTAP는 특정 SMB 공유 이벤트, 특정 감사 정책 이벤트, 특정 로컬 보안 그룹 이벤트, 로컬 사용자 그룹 이벤트 및 인증 정책 이벤트를 비롯한 특정 CLI 변경 이벤트를 감사할 수 있습니다. 감사할 수 있는 변경 이벤트를 이해하면 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

감사 로그를 수동으로 회전하고, 감사를 설정 또는 비활성화하고, 변경 이벤트 감사 정보를 표시하고, 변경 이벤트 감사 및 감사 변경 이벤트를 수정하여, CLI 변경 이벤트를 감사하여 스토리지 가상 시스템(SVM) 감사 CLI 변경 이벤트를 관리할 수 있습니다.

관리자 권한으로 SMB-share, 로컬 사용자 그룹, 로컬 보안 그룹, 인증 정책 및 감사 정책 이벤트와 관련된 구성을 변경하기 위해 명령을 실행하는 경우 레코드가 생성되고 해당 이벤트가 감사됩니다.

감사 범주	이벤트	이벤트 ID입니다	이 명령 실행...
Mhost 감사	정책 변경	[4719] 감사 구성이 변경되었습니다	'vserver audit disable
enable	modify'	파일 공유	[5142] 네트워크 공유가 추가되었습니다
'vserver cifs share create	[5143] 네트워크 공유가 수정되었습니다	'vserver cifs share modify"vserver cifs share create	modify
delete"vserver cifs share add	remove'	[5144] 네트워크 공유가 삭제되었습니다	'vserver cifs share delete
감사	사용자 계정	[4720] 로컬 사용자가 생성되었습니다	'vserver cifs users-and-groups local-user create"vserver services name-service unix-user create'를 참조하십시오
[4722] 로컬 사용자가 활성화되었습니다	'vserver cifs users-and-groups local-user create	modify'를 참조하십시오	[4724] 로컬 사용자 암호 재설정
'vserver cifs users-and-groups local-user set-password	[4725] 로컬 사용자가 비활성화되었습니다	'vserver cifs users-and-groups local-user create	modify'를 참조하십시오
[4726] 로컬 사용자가 삭제되었습니다	'vserver cifs users-and-groups local-user delete"vserver services name-service unix-user delete"를 선택합니다	[4738] 로컬 사용자 변경	'vserver cifs users-and-groups local-user modify"vserver services name-service unix-user modify'를 선택합니다

[4781] 로컬 사용자 이름 바꾸기	'vserver cifs users-and-groups local-user rename'을 선택합니다	보안 그룹	[4731] 로컬 보안 그룹이 생성되었습니다
'vserver cifs users-and-groups local-group create"vserver services name-service unix-group create'를 참조하십시오	[4734] 로컬 보안 그룹이 삭제되었습니다	SVM CIFS 사용자-그룹 로컬-그룹 삭제 SVM 서비스 이름-서비스 UNIX-그룹 삭제	[4735] 로컬 보안 그룹이 수정되었습니다
vserver cifs users-and-groups local-group rename	modify ``vserver services name-service unix-group modify"라는 이름의 가상 서버 사용자 및 그룹 로컬 그룹 이름 변경	[4732] 사용자가 로컬 그룹에 추가되었습니다	가상 CIFS 사용자 및 그룹 로컬 그룹 추가 멤버 가상 서버 서비스 이름 서비스 unix 그룹 추가 사용자
[4733] 사용자가 로컬 그룹에서 제거되었습니다	SVM CIFS 사용자-그룹 local-group remove-멤버들 vserver services name-service unix-group deluser	authorization-policy-change를 참조하십시오	[4704] 사용자 권한이 할당되었습니다
'vserver cifs users-and-groups Privilege add-privilege'	[4705] 사용자 권한이 제거되었습니다	'vserver cifs users-and-groups Privilege remove-Privilege	reset-Privilege

관련 정보

- ["SVM"](#)

파일 공유 ONTAP 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 파일 공유 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다. 파일 공유 이벤트는 SMB 네트워크 공유가 'vserver cifs share' 관련 명령을 사용하여 수정될 때 생성됩니다.

이벤트 ID 5142, 5143 및 5144와 파일 공유 이벤트는 SVM에 대해 SMB 네트워크 공유를 추가, 수정 또는 삭제할 때 생성됩니다. SMB 네트워크 공유 구성은 'CIFS share access control create | modify | delete' 명령을 사용하여 수정합니다.

다음 예에서는 'audit_dest'라는 공유 객체가 생성될 때 ID 5143이 생성된 파일 공유 이벤트를 표시합니다.

```

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)

```

감사 정책 변경 **ONTAP** 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 감사 정책 변경 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다. Audit-policy-change 이벤트는 'vserver audit' 관련 명령어를 이용하여 Audit 정책을 수정할 때 발생합니다.

이벤트 ID 4719를 사용하는 감사 정책 변경 이벤트는 감사 정책이 사용 안 함, 사용 또는 수정될 때마다 생성되며 사용자가 트래킹을 커버하기 위해 감사를 비활성화하려고 시도하는 시점을 식별하는 데 도움이 됩니다. 기본적으로 구성되어 있으며 비활성화하려면 진단 권한이 필요합니다.

다음 예제에서는 감사가 비활성화된 경우 ID 4719가 생성된 감사 정책 변경 이벤트를 표시합니다.

```

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

```

사용자 계정 ONTAP 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 사용자 계정 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4720, 4722, 4724, 4725, 4726, 4738 및 4781은 로컬 SMB 또는 NFS 사용자가 시스템에서 생성 또는 삭제되거나, 로컬 사용자 계정이 활성화, 비활성화 또는 수정되고, 로컬 SMB 사용자 암호가 재설정 또는 변경될 때 생성됩니다. 사용자 계정 이벤트는 사용자 계정이 'vserver cifs users-and-groups_<local user>_' 및 'vserver services name-service_<unix user>_' 명령을 사용하여 수정될 때 생성됩니다.

다음 예에서는 로컬 SMB 사용자가 생성될 때 ID 4720이 생성된 사용자 계정 이벤트를 표시합니다.

```
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 ~
```

다음 예제에서는 앞의 예제에서 만든 로컬 SMB 사용자의 이름이 변경된 경우 ID 4781이 생성된 사용자 계정 이벤트를 표시합니다.

```

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 ~

```

보안 그룹 **ONTAP** 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 보안 그룹 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4731, 4732, 4733, 4734 및 4735가 포함된 보안 그룹 이벤트는 로컬 SMB 또는 NFS 그룹이 시스템에서 생성 또는 삭제되고 로컬 사용자가 그룹에서 추가 또는 제거될 때 생성됩니다. 사용자 계정이 'vserver cifs users-and-groups_<local-group>_' 및 'vserver services name-service_<unix-group>_' 명령을 사용하여 수정될 때 security-group-events가 생성됩니다.

다음 예에서는 로컬 UNIX 보안 그룹이 생성될 때 ID 4731이 생성된 보안 그룹 이벤트를 표시합니다.

```

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 ~

```

authorization-policy-change ONTAP 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 인증 정책 변경 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4704 및 4705의 권한 부여 정책 변경 이벤트는 SMB 사용자 및 SMB 그룹에 대해 권한 부여 권한이 부여되거나 취소될 때마다 생성됩니다. authorization-policy-change 이벤트는 vserver cifs users-and-groups 권한 관련 명령을 사용하여 권한 부여 권한이 할당되거나 취소될 때 생성됩니다.

다음 예에서는 SMB 사용자 그룹에 대한 인증 권한이 할당된 경우 ID 4704가 생성된 인증 정책 이벤트를 표시합니다.

```
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
```

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.