CLI-Änderungsereignisse, die geprüft werden können

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/cli-change-events-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

CLI-Änderungsereignisse, die geprüft werden können 1
Informationen zu ONTAP CLI-Änderungsereignissen, die protokolliert werden können 1
ONTAP Dateifreigabeereignisse verwalten 2
ONTAP-Ereignisse zur Änderung der Audit-Richtlinie verwalten 3
Benutzerkonto-ONTAP-Ereignisse verwalten 4
Verwaltung von ONTAP Sicherheitsgruppen-Ereignissen 5
ONTAP-Ereignisse zur Änderung der Autorisierungsrichtlinie verwalten 6

CLI-Änderungsereignisse, die geprüft werden können

Informationen zu ONTAP CLI-Änderungsereignissen, die protokolliert werden können

ONTAP kann bestimmte CLI-Änderungsereignisse protokollieren, darunter bestimmte SMB-Freigabeereignisse, bestimmte Überwachungsrichtlinienereignisse, bestimmte lokale Sicherheitsgruppenereignisse, lokale Nutzergruppe-Ereignisse und Autorisierungsrichtlinienereignisse. Das Verständnis darüber, welche Änderungsereignisse protokolliert werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Sie können CLI-Änderungsereignisse der Storage Virtual Machine (SVM) verwalten, indem Sie die Audit-Protokolle manuell rotieren, die Auditierung aktivieren oder deaktivieren, Informationen zu Auditierungsänderungsereignissen anzeigen, Auditierungsänderungsereignisse ändern und Auditierungsänderungsereignisse löschen.

Wenn als Administrator ein Befehl ausgeführt wird, der die Konfiguration im Zusammenhang mit SMB-Share, lokaler Nutzergruppe, lokaler Sicherheitsgruppe, Authorization-Policy und Audit-Policy Ereignissen ändert, wird ein Datensatz generiert und das entsprechende Ereignis protokolliert:

Prüfungskategorie	Veranstaltungen	Ereignis-IDs	Führen Sie diesen Befehl aus…
Mhost Auditing	Richtlinienänderung	[4719] Die Audit-Konfiguration wurde geändert	`vserver audit disable
enable	modify`	Dateifreigabe	[5142] Netzwerkfreigabe wurde hinzugefügt
`vserver cifs share create`	[5143] Netzwerkfreigabe wurde geändert	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] Netzwerkfreigabe gelöscht	`vserver cifs share delete`
Prüfung	Benutzerkonto	[4720] Lokaler Nutzer erstellt	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] Lokaler Benutzer aktiviert	`vserver cifs users-and-groups local-user create	modify`	[4724] Zurücksetzen des Passworts des lokalen Benutzers
`vserver cifs users-and-groups local-user set-password`	[4725] Lokaler Benutzer deaktiviert	`vserver cifs users-and-groups local-user create	modify`

[4726] Lokaler Benutzer gelöscht	`vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete`	[4738] Lokale Benutzeränderung	`vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify`
[4781] Lokaler Benutzer umbenennen	`vserver cifs users-and-groups local-user rename`	Sicherheitsgruppe	[4731] Lokale Sicherheitsgruppe erstellt
`vserver cifs users-and-groups local-group create vserver services name-service unix-group create`	[4734] Lokale Sicherheitsgruppe gelöscht	`vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete`	[4735] Lokale Sicherheitsgruppe geändert
`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] Benutzer zur lokalen Gruppe hinzugefügt	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] Benutzer aus lokaler Gruppe entfernt	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	Änderung der Autorisierungsrichtlinie	[4704] Zugewiesene Benutzerrechte
`vserver cifs users-and-groups privilege add-privilege`	[4705] Benutzerrechte entfernt	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

Verwandte Informationen

- "vserver"

ONTAP Dateifreigabeereignisse verwalten

Wenn für eine Storage Virtual Machine (SVM) ein Dateifreigabeereignis konfiguriert und eine Überwachung aktiviert ist, werden Überwachungsereignisse generiert. Die Dateifreigabeereignisse werden generiert, wenn die SMB-Netzwerkfreigabe mit `vserver cifs share` verwandten Befehlen geändert wird.

Die Dateifreigabeereignisse mit den Ereignis-IDs 5142, 5143 und 5144 werden generiert, wenn eine SMB-Netzwerkfreigabe für die SVM hinzugefügt, geändert oder gelöscht wird. Die SMB-Netzwerkfreigabekonfiguration wird mit den `cifs share access control create|modify|delete` Befehlen geändert.

Das folgende Beispiel zeigt ein Dateifreigabeereignis mit der ID 5143, das generiert wird, wenn ein Freigabeobjekt namens 'audit_dest' erstellt wird:

```
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)
```

ONTAP-Ereignisse zur Änderung der Audit-Richtlinie verwalten

Wenn für eine Storage Virtual Machine (SVM) ein Ereignis zur Änderung der Audit-Policy konfiguriert und das Auditing aktiviert ist, werden Audit-Ereignisse generiert. Die Audit-Policy-Change-Ereignisse werden generiert, wenn eine Audit-Policy mithilfe `vserver audit` verwandter Befehle geändert wird.

Das Ereignis „audit-policy-change“ mit der Ereignis-ID 4719 wird immer dann generiert, wenn eine Überwachungsrichtlinie deaktiviert, aktiviert oder geändert wird und hilft dabei, zu erkennen, wenn ein Benutzer versucht, die Überwachung zu deaktivieren, um Spuren zu verwischen. Es ist standardmäßig konfiguriert und erfordert Diagnoseberechtigung zum Deaktivieren.

Das folgende Beispiel zeigt ein Ereignis zur Änderung der Revisionsrichtlinie mit der ID 4719, das generiert wird, wenn eine Überwachung deaktiviert ist:

```
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
```

Benutzerkonto-ONTAP-Ereignisse verwalten

Wenn ein Benutzerkontoereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und eine Überwachung aktiviert ist, werden Überwachungsereignisse generiert.

Die Benutzerkontoereignisse mit den Ereignis-IDs 4720, 4722, 4724, 4725, 4726, 4738 und 4781 werden generiert, wenn ein lokaler SMB- oder NFS-Benutzer im System erstellt oder gelöscht wird, ein lokales Benutzerkonto aktiviert, deaktiviert oder geändert wird oder das Passwort eines lokalen SMB-Benutzers zurückgesetzt oder geändert wird. Die Benutzerkontoereignisse werden generiert, wenn ein Benutzerkonto mithilfe von `vserver cifs users-and-groups <local user>` und `vserver services name-service <unix user>` Befehlen geändert wird.

Das folgende Beispiel zeigt ein Benutzerkontoereignis mit der ID 4720, das generiert wird, wenn ein lokaler SMB-Benutzer erstellt wird:

```
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 ~
```

Das folgende Beispiel zeigt ein Benutzerkontoereignis mit der ID 4781, das generiert wurde, als der im vorhergehenden Beispiel erstellte lokale SMB-Benutzer umbenannt wurde:

```
 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 ~
```

Verwaltung von ONTAP Sicherheitsgruppen-Ereignissen

Wenn ein Sicherheitsgruppenereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und eine Überwachung aktiviert ist, werden Überwachungsereignisse generiert.

Die Sicherheitsgruppenereignisse mit den Ereignis-IDs 4731, 4732, 4733, 4734 und 4735 werden generiert, wenn eine lokale SMB- oder NFS-Gruppe auf dem System erstellt oder gelöscht wird und ein lokaler Benutzer der Gruppe hinzugefügt oder daraus entfernt wird. Die Sicherheitsgruppenereignisse werden generiert, wenn ein Benutzerkonto mit `vserver cifs users-and-groups <local-group>`- und `vserver services name-service <unix-group>`-Befehlen geändert wird.

Das folgende Beispiel zeigt ein Sicherheitsgruppenereignis mit der ID 4731, das beim Erstellen einer lokalen UNIX-Sicherheitsgruppe generiert wird:

```
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 ~
```

ONTAP-Ereignisse zur Änderung der Autorisierungsrichtlinie verwalten

Wenn das Ereignis zur Änderung der Autorisierungsrichtlinie für eine Storage Virtual Machine (SVM) konfiguriert ist und eine Revisionsfunktion aktiviert ist, werden Revisionsereignisse generiert.

Die Ereignisse vom Typ „Autorisierungsrichtlinienänderung“ mit den Ereignis-IDs 4704 und 4705 werden immer dann generiert, wenn einem SMB-Benutzer oder einer SMB-Gruppe Autorisierungsrechte erteilt oder entzogen werden. Die Ereignisse vom Typ „Autorisierungsrichtlinienänderung“ werden generiert, wenn die Autorisierungsrechte mithilfe von `vserver cifs users-and-groups privilege` zugehörigen Befehlen zugewiesen oder entzogen werden.

Das folgende Beispiel zeigt ein Autorisierungsrichtlinienereignis mit der ID 4704, das generiert wurde, als die Autorisierungsrechte für eine SMB-Benutzergruppe zugewiesen wurden:

```
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
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.