



Änderungsereignisse in der CLI, die geprüft werden können

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Änderungsereignisse in der CLI, die geprüft werden können 1
 - Änderungsereignisse in der CLI, die geprüft werden können, Übersicht 1
 - Dateifreigabe-Ereignisse verwalten 2
 - Management von Änderungs- und Audit-Richtlinien 3
 - Verwalten von Benutzerkontenereignis 4
 - Verwalten von Sicherheitsereignisereignis 6
 - Management von Berechtigungs- und Richtlinienänderungen 7

Änderungsereignisse in der CLI, die geprüft werden können

Änderungsereignisse in der CLI, die geprüft werden können, Übersicht

ONTAP kann bestimmte CLI-Änderungsereignisse prüfen, darunter bestimmte SMB-Share-Ereignisse, bestimmte Audit-Richtlinienereignisse, bestimmte lokale Ereignisse von Sicherheitsgruppen, Ereignisse lokaler Benutzergruppen und Autorisierungsrichtlinien. Das Verständnis, welche Änderungsereignisse überprüft werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Sie können die Ereignisse, die auf einer Storage Virtual Machine (SVM) stattfinden, verwalten, indem Sie die Überwachungsprotokolle manuell drehen, die Prüfung aktivieren oder deaktivieren, Informationen über das Auditing von Änderungsereignissen anzeigen, Änderungsereignisse für das Auditing ändern und Änderungsereignisse für das Auditing löschen.

Wenn Sie als Administrator einen beliebigen Befehl zum Ändern der Konfiguration in Bezug auf SMB-Share, lokale Benutzergruppe, lokale Sicherheitsgruppe, Autorisierungsrichtlinie und Ereignis für Prüfrichtlinien ausführen, Ein Datensatz erzeugt und das entsprechende Ereignis wird auditiert:

Kategorie „Audits“	Veranstaltungen	Ereignis-IDs	Führen Sie diesen Befehl aus...
Mhost Auditing	Richtlinienänderung	[4719] Audit-Konfiguration 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 Benutzer 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 lokalen Benutzerpassworts

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 der lokalen Gruppe entfernt	vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser	Änderung der Autorisierungsrichtlinie	[4704] Benutzerrechte Zugewiesen
vserver cifs users-and-groups privilege add-privilege	[4705] Benutzerrechte Entfernt	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

Dateifreigabe-Ereignisse verwalten

Wenn ein Dateifreigabe-Ereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert. Die Dateifreigabe-Ereignisse werden generiert, wenn die SMB-Netzwerkfreigabe mit geändert wird

`vserver cifs share` Ähnliche Befehle.

Die Dateifreigabe-Ereignisse mit den Ereignis-ids 5142, 5143 und 5144 werden generiert, wenn eine SMB-Netzwerkfreigabe für die SVM hinzugefügt, geändert oder gelöscht wird. Die Konfiguration der SMB-Netzwerkfreigabe wird mithilfe des geändert `cifs share access control create|modify|delete` Befehle.

Im folgenden Beispiel wird ein Dateifreigabe-Ereignis mit der ID 5143 erzeugt, wenn ein Freigabetobjekt 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)
```

Management von Änderungs- und Audit-Richtlinien

Wenn ein Ereignis für die Änderung von Audit-Richtlinien für eine Storage Virtual Machine (SVM) konfiguriert und ein Audit aktiviert ist, werden Audit-Ereignisse generiert. Die Ereignisse der Revisionspolitik-Änderung werden generiert, wenn eine Audit-Richtlinie mit geändert wird `vserver audit` Ähnliche Befehle.

Das Ereignis „Audit-Policy-change“ mit der Ereignis Event-id 4719 wird immer dann generiert, wenn eine Audit-Richtlinie deaktiviert, aktiviert oder geändert wird. Außerdem wird festgestellt, wann ein Benutzer versucht, die Prüfung für die Tracks zu deaktivieren. Er ist standardmäßig konfiguriert und erfordert zum Deaktivieren Diagnoseberechtigung.

Im folgenden Beispiel wird ein Änderungsereignis für die Audit-Richtlinie mit der generierten ID 4719 angezeigt, wenn ein Audit 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

```

Verwalten von Benutzerkontenereignis

Wenn ein Benutzerkontenereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Ereignisse des Benutzerkontos mit Event-ids 4720, 4722, 4724, 4725, 4726 4738 und 4781 werden generiert, wenn ein lokaler SMB- oder NFS-Benutzer aus dem System erstellt oder gelöscht wird, ein lokales Benutzerkonto ist aktiviert, deaktiviert oder geändert und das lokale SMB-Benutzerpasswort wird zurückgesetzt oder geändert. Die Benutzerkontoereignisse werden generiert, wenn ein Benutzerkonto mit `vserver cifs users-and-groups <local user>` Und `vserver services name-service <unix user>` Befehle.

Im folgenden Beispiel wird ein Benutzerkontoereignis mit der ID 4720 angezeigt, das beim Erstellen eines lokalen SMB-Benutzers generiert wurde:

```

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 ~

```

Im folgenden Beispiel wird ein Benutzerkontoereignis mit der anhand der ID 4781 erstellten ID angezeigt, wenn der im vorhergehenden Beispiel erstellte lokale SMB-Benutzer umbenannt wird:

```

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 ~

```

Verwalten von Sicherheitereignisereignis

Wenn ein Sicherheitereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Die Ereignisse der Sicherheitsgruppe mit Ereignis-ids 4731, 4732, 4733, 4734 und 4735 werden generiert, wenn eine lokale SMB- oder NFS-Gruppe aus dem System erstellt oder gelöscht wird und der lokale Benutzer aus der Gruppe hinzugefügt oder entfernt wird. Die Ereignisse der Sicherheitsgruppe werden generiert, wenn ein Benutzerkonto mit geändert wird `vserver cifs users-and-groups <local-group>` Und `vserver services name-service <unix-group>` Befehle.

Im folgenden Beispiel wird ein Ereignis der Sicherheitsgruppe mit der generierten ID 4731 angezeigt, wenn eine lokale UNIX-Sicherheitsgruppe erstellt 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 ~

```

Management von Berechtigungs- und Richtlinienänderungen

Wenn ein Ereignis zur Änderung von Autorisierungsrichtlinien für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Die Ereignisse mit den Ereignis-ids 4704 und 4705 werden generiert, sobald die Autorisierungsrechte für einen SMB-Benutzer und eine SMB-Gruppe erteilt oder widerrufen werden. Die Ereignisse zur Änderung der Autorisierungsrichtlinie werden generiert, wenn die Autorisierungsrechte mit zugewiesen oder widerrufen werden `vserver cifs users-and-groups privilege` Ähnliche Befehle.

Im folgenden Beispiel wird ein Ereignis für die Autorisierungsrichtlinie mit der generierten ID 4704 angezeigt, wenn die Autorisierungsrechte für eine SMB-Benutzergruppe zugewiesen sind:

```
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 © 2024 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 IRGEND EINER 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.