Informationen zu den auf Dateien und Verzeichnisse angewendeten Revisionsrichtlinien

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/display-audit-policies-windows-security-tab-task.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Informationen zu den auf Dateien und Verzeichnisse angewendeten Revisionsrichtlinien 1
Informationen zu den ONTAP-Revisionsrichtlinien sind über die Registerkarte „Windows-Sicherheit“ einsehbar. 1
Informationen zu NTFS-Audit-Richtlinien auf ONTAP FlexVol Volumes 2
Platzhalterzeichen können verwendet werden, um Informationen zu ONTAP Dateisicherheits- und Revisionsprotokollrichtlinien anzuzeigen. 5

Informationen zu den auf Dateien und Verzeichnisse angewendeten Revisionsrichtlinien

Informationen zu den ONTAP-Revisionsrichtlinien sind über die Registerkarte „Windows-Sicherheit“ einsehbar.

Informationen zu den auf Dateien und Verzeichnisse angewendeten Revisionsrichtlinien werden über die Registerkarte „Sicherheit“ im Eigenschaftenfenster von Windows angezeigt. Dies ist die gleiche Methode wie für Daten auf einem Windows Server, wodurch Kunden die gewohnte GUI-Oberfläche nutzen können.

Über diese Aufgabe

Die Anzeige von Informationen über auf Dateien und Verzeichnisse angewendete Revisionsrichtlinien ermöglicht die Überprüfung, ob die entsprechenden Systemzugriffskontrolllisten (SACLs) für bestimmte Dateien und Ordner festgelegt sind.

Informationen über SACLs, die auf NTFS-Dateien und Ordner angewendet wurden, lassen sich auf einem Windows-Host wie folgt anzeigen.

Schritte

1. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
2. Das Dialogfeld **Netzlaufwerk verbinden** ausfüllen:

   a. Einen Laufwerksbuchstaben auswählen.

   b. Im Feld **Ordner** ist die IP-Adresse oder der SMB-Servername der Storage Virtual Machine (SVM) anzugeben, die die Freigabe enthält, welche sowohl die zu prüfenden Daten als auch den Namen der Freigabe enthält.

      Wenn Ihr SMB-Servername “SMB_SERVER” ist und Ihre Freigabe “share1” heißt, sollte `\\SMB_SERVER\share1` eingegeben werden.

      Sie können die IP-Adresse der Datenschnittstelle für den SMB-Server anstelle des SMB-Servernamens angeben.

   c. Klicken Sie auf **Finish**.

   Das von Ihnen ausgewählte Laufwerk ist eingebunden und einsatzbereit, wobei das Windows Explorer-Fenster die in der Freigabe enthaltenen Dateien und Ordner anzeigt.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das Überwachungsinformationen angezeigt werden.
4. Mit der rechten Maustaste auf die Datei oder das Verzeichnis klicken und **Eigenschaften** auswählen.
5. Die Registerkarte **Sicherheit** auswählen.
6. Auf **Erweitert** klicken.
7. Die Registerkarte **Überwachung** auswählen.
8. Klicken Sie auf **Weiter**.

Das Überwachungsfenster öffnet sich. Im Fenster **Überwachungseinträge** wird eine Zusammenfassung der Benutzer und Gruppen angezeigt, denen SACLs zugewiesen sind.

9. Im Feld **Überwachungseinträge** den Benutzer oder die Gruppe auswählen, deren SACL-Einträge angezeigt werden sollen.
10. Klicken Sie auf **Bearbeiten**.

    Der Auditing-Eintrag für <object> wird geöffnet.

11. Im Feld **Zugriff** werden die aktuell auf das ausgewählte Objekt angewendeten SACLs angezeigt.
12. Klicken Sie auf **Abbrechen**, um das Feld **Überwachungseintrag für <object>** zu schließen.
13. Mit **Abbrechen** wird das Fenster **Überwachung** geschlossen.

Informationen zu NTFS-Audit-Richtlinien auf ONTAP FlexVol Volumes

Sie können Informationen zu NTFS-Überwachungsrichtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten. Diese Informationen dienen zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen.

Über diese Aufgabe

Die Anzeige von Informationen über auf Dateien und Verzeichnisse angewendete Revisionsrichtlinien ermöglicht die Überprüfung, ob die entsprechenden Systemzugriffskontrolllisten (SACLs) für bestimmte Dateien und Ordner festgelegt sind.

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- NTFS Security-Style Volumes und Qtrees verwenden ausschließlich NTFS-Systemzugriffskontrolllisten (SACLs) für Audit-Richtlinien.
- Auf Dateien und Ordner in einem Volume mit gemischtem Sicherheitsstil und effektiver NTFS-Sicherheit können NTFS-Überwachungsrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NTFS-SACLs enthalten oder auch nicht.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei- und Ordner-NFSv4-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS effektiver Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

- Bei der Anzeige von Sicherheitsinformationen zu Dateien und Ordnern mit NTFS effektiver Sicherheit enthalten die UNIX-bezogenen Ausgabefelder nur Anzeigeinformationen zu UNIX-Dateiberechtigungen.

  Dateien und Ordner im NTFS-Sicherheitsstil verwenden ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte.

- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige der Überwachungsrichtlinieneinstellungen für Dateien und Verzeichnisse mit dem gewünschten Detaillierungsgrad:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Als detaillierte Liste	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/corp` in SVM vs1. Der Pfad verfügt über effektive NTFS-Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen SUCCESS- als auch einen SUCCESS/FAIL-SACL-Eintrag.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
```

```
                            ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                            SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                          DACL - ACEs
                            ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                            ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                            ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/datavol1` in SVM vs1. Der Pfad enthält sowohl reguläre Datei- und Ordner-SACLs als auch Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
```

```
                            AUDIT-EXAMPLE\Domain Users-0x120089-FA
                            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                          DACL (Applies to Files):
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-EXAMPLE\engineering-0x1f01ff
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Platzhalterzeichen können verwendet werden, um Informationen zu ONTAP Dateisicherheits- und Revisionsprotokollrichtlinien anzuzeigen.

Sie können das Platzhalterzeichen (*) verwenden, um Informationen über die Dateisicherheit und die Revisionsprotokollrichtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Stammvolume anzuzeigen.

Das Platzhalterzeichen (*) kann als letzter Bestandteil eines angegebenen Verzeichnispfads verwendet werden, unterhalb dessen Informationen zu allen Dateien und Verzeichnissen angezeigt werden.

Wenn Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen "*" angezeigt werden sollen, ist der vollständige Pfad in doppelten Anführungszeichen (" ") anzugeben.

Beispiel

Der folgende Befehl mit dem Platzhalterzeichen zeigt die Informationen zu allen Dateien und Verzeichnissen unterhalb des Pfads `/1/` von SVM vs1 an:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
          Security Style: mixed
         Effective Style: ntfs
          DOS Attributes: 10
     DOS Attributes in Text: ----D---
   Expanded Dos Attributes: -
            Unix User Id: 0
           Unix Group Id: 0
          Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                     ACLs: NTFS Security Descriptor
                           Control:0x8514
                           Owner:BUILTIN\Administrators
                           Group:BUILTIN\Administrators
                           DACL - ACEs
                           ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                  Vserver: vs1
```

```
                 File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Der folgende Befehl zeigt die Informationen einer Datei mit dem Namen "*" unter dem Pfad `/vol1/a` von SVM vs1 an. Der Pfad ist in doppelte Anführungszeichen (" ") eingeschlossen.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

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.