



Informationen über auf Dateien und Verzeichnisse angewandte Audit-Richtlinien anzeigen

ONTAP 9

NetApp
February 12, 2026

Inhalt

- Informationen über auf Dateien und Verzeichnisse angewandte Audit-Richtlinien anzeigen 1
 - Zeigen Sie Informationen zu ONTAP-Überwachungsrichtlinien an, indem Sie auf die Registerkarte Windows-Sicherheit zugreifen 1
 - Zeigt Informationen über NTFS-Überwachungsrichtlinien auf ONTAP FlexVol-Volumes an 2
 - Verwenden Sie Platzhalterzeichen, um Informationen zu ONTAP-Dateisicherheit und Audit-Richtlinien anzuzeigen 6

Informationen über auf Dateien und Verzeichnisse angewandte Audit-Richtlinien anzeigen

Zeigen Sie Informationen zu ONTAP-Überwachungsrichtlinien an, indem Sie auf die Registerkarte Windows-Sicherheit zugreifen

Sie können Informationen zu Audit-Richtlinien anzeigen, die auf Dateien und Verzeichnisse angewendet wurden, indem Sie die Registerkarte Sicherheit im Fenster Windows-Eigenschaften verwenden. Das ist dieselbe Methode für Daten auf einem Windows Server, mit der Kunden dieselbe Benutzeroberfläche nutzen können, die sie bereits kennen.

Über diese Aufgabe

Durch das Anzeigen von Informationen über Überwachungsrichtlinien, die auf Dateien und Verzeichnisse angewendet werden, können Sie überprüfen, ob die entsprechenden SACs (System Access Control Lists) für bestimmte Dateien und Ordner festgelegt sind.

Führen Sie die folgenden Schritte auf einem Windows-Host aus, um Informationen über SACs anzuzeigen, die auf NTFS-Dateien und -Ordner angewendet wurden.

Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie das Dialogfeld **Map Network Drive** aus:
 - a. Wählen Sie einen **Drive**-Buchstaben aus.
 - b. Geben Sie im Feld **Ordner** die IP-Adresse oder den Namen des SMB-Servers der virtuellen Speichermaschine (SVM) ein, die den Share enthält, der sowohl die zu prüfenden Daten als auch den Namen der Freigabe enthält.

Wenn Ihr SMB-Servername „SMB_SERVER“ lautet und Ihre Freigabe den Namen „share1“ hat, sollten Sie eingeben \\SMB_SERVER\share1.



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

- c. Klicken Sie Auf **Fertig Stellen**.

Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das Sie Audit-Informationen anzeigen.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie **Eigenschaften**.
5. Wählen Sie die Registerkarte **Sicherheit**.
6. Klicken Sie Auf **Erweitert**.

7. Wählen Sie die Registerkarte **Revision** aus.

8. Klicken Sie Auf **Weiter**.

Das Feld Auditing wird geöffnet. Das Feld * Revisionseinträge* zeigt eine Zusammenfassung von Benutzern und Gruppen an, deren SACLS auf sie angewendet wurden.

9. Wählen Sie im Feld * Überwachungseinträge* den Benutzer oder die Gruppe aus, deren SACL-Einträge angezeigt werden sollen.

10. Klicken Sie Auf **Bearbeiten**.

Der Überwachungseintrag für <object> wird geöffnet.

11. Zeigen Sie im Feld **Zugriff** die aktuellen SACLS an, die auf das ausgewählte Objekt angewendet werden.

12. Klicken Sie auf **Abbrechen**, um das Feld **Prüfeintrag für <Object>** zu schließen.

13. Klicken Sie auf **Abbrechen**, um das Feld **Revision** zu schließen.

Zeigt Informationen über NTFS-Überwachungsrichtlinien auf ONTAP FlexVol-Volumes an

Sie können Informationen zu NTFS-Audit-Richtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu Zugriffssteuerungslisten des Systems. Sie können die Informationen zur Überprüfung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Audit-Problemen verwenden.

Über diese Aufgabe

Durch das Anzeigen von Informationen über Überwachungsrichtlinien, die auf Dateien und Verzeichnisse angewendet werden, können Sie überprüfen, ob die entsprechenden SACLS (System Access Control Lists) 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 angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Bei NTFS-Volumes und qtrees werden für Audit-Richtlinien nur NTFS-Systemzugriffssteuerungslisten (SACLS) verwendet.
- Dateien und Ordner in einem gemischten Security-Stil-Volume mit NTFS effektive Sicherheit können NTFS-Audit-Richtlinien auf sie angewendet werden.

Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und möglicherweise NTFS SACLS enthalten.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale Datei als auch Ordner NFSv4 SACLS und Storage-Level Access Guard NTFS SACLS an.

- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Wenn Sicherheitsinformationen über Dateien und Ordner mit NTFS-effektiver Sicherheit angezeigt werden, enthalten UNIX-bezogene Ausgabefelder nur Informationen über die Berechtigung von UNIX-Dateien.

NTFS-Dateien und -Ordner verwenden bei der Ermittlung der Zugriffsrechte auf Dateien nur NTFS-Dateiberechtigungen und Windows-Benutzer und -Gruppen.

- 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, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige von Datei- und Verzeichnisaudits-Einstellungen mit der gewünschten Detailebene:

Informationen anzeigen...	Geben Sie den folgenden Befehl ein...
In zusammengefassener Form	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Als detaillierte Liste	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Beispiele

Im folgenden Beispiel werden die Informationen der Überwachungsrichtlinie für den Pfad `/corp` in SVM `vs1` angezeigt. Der Pfad verfügt über NTFS effektive Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen ERFOLG als auch einen SACL-Eintrag FÜR ERFOLG/FEHLER.

```

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

```

Im folgenden Beispiel werden die Informationen der Überwachungsrichtlinie für den Pfad /datavol1 in SVM vs1 angezeigt. Der Pfad enthält sowohl normale Datei- als auch Ordner-SACLs und Speicher-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
```

Verwenden Sie Platzhalterzeichen, um Informationen zu ONTAP-Dateisicherheit und Audit-Richtlinien anzuzeigen

Mithilfe des Platzhalterzeichens (*) können Sie Informationen über Dateisicherheit und Audit-Richtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Root-Volume anzeigen.

Das Platzhalterzeichen (*) kann als letzte Unterkomponente eines bestimmten Verzeichnispfades verwendet werden, unter dem Sie Informationen zu allen Dateien und Verzeichnissen anzeigen möchten.

Wenn Sie Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „*“ anzeigen möchten, müssen Sie den vollständigen Pfad innerhalb doppelter Anführungszeichen („ “) angeben.

Beispiel

Mit dem folgenden Befehl mit dem Platzhalterzeichen werden die Informationen zu allen Dateien und Verzeichnissen unterhalb des Pfades von /1/ SVM vs1 angezeigt:


```

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)

```

Mit dem folgenden Befehl werden die Informationen einer Datei mit dem Namen „*“ unter dem Pfad /vol1/a von SVM vs1 angezeigt. 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 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.