Informationen zu Dateisicherheit und Überwachungsrichtlinien

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/display-file-security-audit-policies-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Informationen zu Dateisicherheit und Überwachungsrichtlinien . . . 1
- Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien . . . 1
  - Anzeige von Informationen zur Dateisicherheit . . . 1
  - Anzeige von Informationen über Prüfungsrichtlinien . . . 1
  - Anzeige von Informationen zur Storage-Level Access Guard (SLAG) Sicherheit . . . 1
  - Anzeigen von Informationen zur Dynamic Access Control (DAC) Sicherheit . . . 1
- Informationen zur ONTAP SMB-Dateisicherheit auf NTFS Security-Style-Volumes anzeigen . . . 2
- Informationen zur ONTAP SMB-Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen . . . 7
- Informationen zur ONTAP SMB-Dateisicherheit auf UNIX Security-Style-Volumes anzeigen . . . 10
- ONTAP Befehle zur Anzeige von Informationen über NTFS-Überwachungsrichtlinien auf SMB FlexVol Volumes . . . 12
- ONTAP Befehle zur Anzeige von Informationen zu NFSv4-Überwachungsrichtlinien auf SMB FlexVol volumes . . . 15
- Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien . . . 16

Informationen zu Dateisicherheit und Überwachungsrichtlinien

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

Informationen zur Dateisicherheit von Dateien und Verzeichnissen in Volumes auf Storage Virtual Machines (SVMs) können angezeigt werden. Informationen zu Überwachungsrichtlinien auf FlexVol volumes können angezeigt werden. Wenn konfiguriert, können Informationen zu Storage-Level Access Guard und Dynamic Access Control Sicherheitseinstellungen auf FlexVol volumes angezeigt werden.

Anzeige von Informationen zur Dateisicherheit

Es lassen sich Informationen über die auf Daten in Volumes und Qtrees (für FlexVol volumes) angewendete Dateisicherheit mit den folgenden Sicherheitsstilen anzeigen:

- NTFS
- UNIX
- Gemischt

Anzeige von Informationen über Prüfungsrichtlinien

Informationen zu Überwachungsrichtlinien für die Überwachung von Zugriffsereignissen auf FlexVol volumes über die folgenden NAS-Protokolle können angezeigt werden:

- SMB (alle Versionen)
- NFSv4.x

Anzeige von Informationen zur Storage-Level Access Guard (SLAG) Sicherheit

Die Storage-Level Access Guard-Sicherheit kann auf FlexVol volumes und qtree-Objekte mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt
- UNIX (wenn auf der SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist)

Anzeigen von Informationen zur Dynamic Access Control (DAC) Sicherheit

Die Dynamic Access Control-Sicherheit kann auf ein Objekt innerhalb eines FlexVol volume mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt (wenn das Objekt über effektive NTFS-Sicherheit verfügt)

Verwandte Informationen

- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard
- Informationen zu Storage-Level Access Guard auf Servern

Informationen zur ONTAP SMB-Dateisicherheit auf NTFS Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf NTFS-Sicherheitsstil-Volumes anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu DOS-Attributen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

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

- Da NTFS Security-Style Volumes und Qtrees ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte verwenden, enthalten UNIX-bezogene Ausgabefelder lediglich zur Anzeige bestimmte UNIX-Dateiberechtigungsinformationen.
- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Storage-Level Access Guard Sicherheit auf dem Volume-Root oder Qtree konfiguriert werden kann, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei-ACLs als auch Storage-Level Access Guard ACLs anzeigen.
- Die Ausgabe zeigt außerdem Informationen über die ACEs der Dynamic Access Control an, falls Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/vol4` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         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:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Das folgende Beispiel zeigt die Sicherheitsinformationen mit erweiterten Masken zum Pfad `/data/engineering` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
```

```
                            1... .... .... .... = Self Relative
                            .0.. .... .... .... = RM Control Valid
                            ..0. .... .... .... = SACL Protected
                            ...0 .... .... .... = DACL Protected
                            .... 0... .... .... = SACL Inherited
                            .... .0.. .... .... = DACL Inherited
                            .... ..0. .... .... = SACL Inherit Required
                            .... ...0 .... .... = DACL Inherit Required
                            .... .... ..0. .... = SACL Defaulted
                            .... .... ...0 .... = SACL Present
                            .... .... .... 0... = DACL Defaulted
                            .... .... .... .1.. = DACL Present
                            .... .... .... ..0. = Group Defaulted
                            .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
```

```
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
```

```
                            .... .... .... .... .... .... .... .0.. =
Append
                            .... .... .... .... .... .... .... ..0. =
Write
                            .... .... .... .... .... .... .... ...0 =
Read
```

Das folgende Beispiel zeigt Sicherheitsinformationen, einschließlich Storage-Level Access Guard-Sicherheitsinformationen, für das Volume mit dem Pfad `/datavol1` in SVM vs1:

```
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:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         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
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

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

- Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Ordner 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 effektive UNIX- oder NTFS-Sicherheit haben.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, 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.
- 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 UNIX-Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit effektiver NTFS-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.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

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

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/projects` in SVM vs1 in erweiterter Maskenform. Dieser Pfad mit gemischtem Security-Style hat effektive UNIX-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/data` in SVM vs1. Dieser Pfad mit gemischtem Sicherheitsstil hat eine effektive NTFS-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         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:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Volume am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Mixed Security-Style Volumes verfügt über effektive UNIX-Sicherheit. Das Volume verfügt über Storage-Level Access Guard-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
```

```
                            ALLOW-EXAMPLE\market-0x1f01ff
                          SACL (Applies to Files):
                            AUDIT-EXAMPLE\Domain Users-0x120089-FA
                            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                            AUDIT-EXAMPLE\market-0x1f01ff-SA
                          DACL (Applies to Files):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-EXAMPLE\engineering-0x1f01ff
                            ALLOW-EXAMPLE\market-0x1f01ff
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf NTFS Security-Style-Volumes
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf UNIX Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf UNIX Security-Style-Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und -Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Verzeichnissicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- UNIX Security-Style-Volumes und Qtrees verwenden zur Bestimmung der Dateizugriffsrechte ausschließlich UNIX-Dateiberechtigungen, entweder Modusbits oder NFSv4-ACLs.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NFSv4-Sicherheit angezeigt.

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

- Die Ausgabefelder „Eigentümer“ und „Gruppe“ in der ACL-Ausgabe gelten nicht für NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren aussagekräftig.

- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

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

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/home` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/home` in SVM vs1 in erweiterter Maskenform:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
```

```
                        .... .... ..0. .... = Archive
                        .... .... ...1 .... = Directory
                        .... .... .... .0.. = System
                        .... .... .... ..0. = Hidden
                        .... .... .... ...0 = Read Only
                              Unix User Id: 0
                             Unix Group Id: 1
                            Unix Mode Bits: 700
                    Unix Mode Bits in Text: rwx------
                                      ACLs: -
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf Security-Style-Volumes anzeigen
- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

ONTAP Befehle zur Anzeige von Informationen über NTFS-Überwachungsrichtlinien auf SMB 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. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

Über diese Aufgabe

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
```

ONTAP Befehle zur Anzeige von Informationen zu NFSv4-Überwachungsrichtlinien auf SMB FlexVol volumes

Es lassen sich Informationen zu NFSv4-Auditrichtlinien auf FlexVol volumes mithilfe der ONTAP CLI anzeigen, darunter die Sicherheitsstile und effektiven Sicherheitsstile, die angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten (SACLs). Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

Über diese Aufgabe

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

- UNIX Security-Style Volumes und Qtrees verwenden ausschließlich NFSv4 SACLs für Audit-Richtlinien.
- Auf Dateien und Verzeichnisse in einem Volume mit gemischtem Sicherheitsstil, die dem UNIX-Sicherheitsstil entsprechen, können NFSv4-Auditrichtlinien 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 NFSv4-SACLs enthalten oder auch nicht.
- 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.
- 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 NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritte

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

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

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/lab` in SVM vs1. Dieser UNIX-Sicherheitsstil-Pfad verfügt über eine NFSv4-SACL.

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

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 doppelte 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.