Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/display-file-security-audit-policies-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

Inhalt

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an . . . 1
Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an . . . 1
Zeigt Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes an . . . 2
Zeigt Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart an . . . 8
Anzeige von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil . . . 11
Zeigt Informationen zu NTFS-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an . . . 14
Zeigt Informationen über die NFSv4-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an . . . 17
Möglichkeiten zum Anzeigen von Informationen über Dateisicherheitsrichtlinien und Audit-Richtlinien . . . 18

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Sie können Informationen zur Dateisicherheit auf Dateien und Verzeichnissen in Volumes auf Storage Virtual Machines (SVMs) anzeigen. Sie können Informationen zu Audit-Richtlinien in FlexVol Volumes anzeigen. Wenn konfiguriert, können Sie Informationen über die Sicherheitseinstellungen der Speicherebene und der dynamischen Zugriffskontrolle auf FlexVol Volumes anzeigen.

Anzeigen von Informationen zur Dateisicherheit

Sie können Informationen zur Dateisicherheit auf Daten anzeigen, die in Volumes und qtrees (für FlexVol Volumes) enthalten sind. Hierzu zählen folgende Sicherheitsstile:

- NTFS
- UNIX
- Gemischt

Anzeigen von Informationen zu Audit-Richtlinien

Sie können Informationen zu Audit-Richtlinien für das Auditing von Zugriffsereignissen auf FlexVol Volumes über die folgenden NAS-Protokolle anzeigen:

- SMB (alle Versionen)
- NFSv4.x

Anzeigen von Informationen zur Sicherheit des Storage-Level Access Guard (SCHLACKE)

Die Sicherheit des Zugriffschutzes auf Storage-Ebene kann auf FlexVol Volumes und qtree Objekte mit den folgenden Sicherheitsstilen angewendet werden:

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

Anzeigen von Informationen zur DAC-Sicherheit (Dynamic Access Control

Die Sicherheit der dynamischen Zugriffssteuerung lässt sich auf ein Objekt innerhalb eines FlexVol-Volumes anwenden:

- NTFS
- Gemischt (wenn das Objekt NTFS-effektive Sicherheit hat)

Verwandte Informationen

Dateizugriff wird mithilfe von Storage-Level Access Guard gesichert

Anzeigen von Informationen zum Speicher-Level Access Guard

Zeigt Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes an

Sie können Informationen über die Datei- und Verzeichnissicherheit auf NTFS-Volumes im Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen über DOS-Attribute. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Da NTFS Security-Style Volumes und qtrees bei der Ermittlung von Dateizugriffsrechten nur NTFS-Dateiberechtigungen und Windows-Benutzer sowie -Gruppen verwenden, enthalten UNIX-bezogene Ausgabefelder nur Informationen zu Bildschirmberechtigungen für UNIX-Dateien.
- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Sicherheit des Storage-Level Access Guard im Root-Verzeichnis oder qtree konfiguriert werden kann, wird die Ausgabe für einen Volume- oder qtree-Pfad, wo der Storage-Level Access Guard konfiguriert ist, möglicherweise sowohl normale Datei-ACLs als auch Storage-Level Access Guard ACLs angezeigt.
- Die Ausgabe zeigt auch Informationen zu dynamischen Zugriffssteuerungsassen an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/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
```

Im folgenden Beispiel werden die Sicherheitsinformationen mit erweiterten Masken zum Pfad angezeigt `/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
```

Im folgenden Beispiel werden Sicherheitsinformationen für das Volume mit dem Pfad angezeigt, einschließlich Sicherheitsinformationen auf Storage-Ebene Access Guard `/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

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Zeigt Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart an

Sie können Informationen über die Datei- und Verzeichnissicherheit auf Volumes mit gemischter Sicherheitsart anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu UNIX-Eigentümern und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Ordner 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 Volumes im Sicherheitsstil kann entweder UNIX oder NTFS effektiven Schutz 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, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).
- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.
- 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, kann möglicherweise sowohl UNIX Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- 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.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/projects` In SVM vs1 als erweiterte Maske. Dieser Pfad im gemischten Sicherheitsstil verfügt über 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: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/data` In SVM vs1. Dieser Pfad mit gemischtem Sicherheitsstil verfügt über eine NTFS-effektive 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
```

Im folgenden Beispiel werden die Sicherheitsinformationen zum Volume im Pfad angezeigt `/datavol5` In SVM vs1. Auf der obersten Ebene dieses gemischten Volumes im Sicherheitsstil ist UNIX effektive Sicherheit. Das Volume verfügt über Sicherheit auf Storage-Ebene beim Access Guard.

```
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

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Anzeige von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Sie können Informationen über die Datei- und Verzeichnissicherheit auf UNIX-Volumes

im Sicherheitsstil anzeigen, einschließlich der Sicherheitsstile und der effektiven Sicherheitsstile, welche Berechtigungen angewendet werden, sowie Informationen über UNIX-Besitzer und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für die Datei oder das Verzeichnis angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX-Volumes und qtrees verwenden beim Bestimmen von Dateizugriffsrechten nur UNIX-Dateiberechtigungen, entweder Mode-Bits 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, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder für die Ausgabe der Eigentümer und der Gruppen in der ACL gelten nicht bei NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren sinnvoll.

- Da die Sicherheit des Storage-Level Access Guard auf einem UNIX Volume oder qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die Sicherheit des Storage-Level Access Guard enthalten, der auf dem angegebenen Volume oder qtree im angewendet wird `-path` Parameter.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/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: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/home` In SVM vs1 als erweiterte Maske:

```
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

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Zeigt Informationen zu NTFS-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI 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 Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

Über diese Aufgabe

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	`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

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt `/corp` In SVM vs1. 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 zu den Überwachungsrichtlinien für den Pfad angezeigt

`/datavol1` In SVM vs1. 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
```

Zeigt Informationen über die NFSv4-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an

Sie können Informationen über NFSv4-Audit-Richtlinien auf FlexVol-Volumes über die ONTAP-CLI anzeigen, einschließlich der Sicherheitsstile und des effektiven Sicherheitsstyles, der angewandten Berechtigungen und Informationen zu Systemzugriffssteuerungslisten (SACLs). Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

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. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX Volumes und qtrees im Sicherheitsstil verwenden ausschließlich NFSv4 SACLs für Prüfrichtlinien.
- Dateien und Verzeichnisse in einem gemischten Volume mit Sicherheitsstil, das sich im UNIX-Sicherheitsstil befinden, können NFSv4-Audit-Richtlinien auf sie anwenden.

  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 darf NFSv4 SACLs nicht enthalten.
- 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.
- 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 NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS SACLs an.
- Da die Sicherheit des Storage-Level Access Guard auf einem UNIX Volume oder qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die Sicherheit des Storage-Level Access Guard enthalten, der auf dem angegebenen Volume oder qtree im angewendet wird `-path` Parameter.

Schritte

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/lab` In SVM vs1. Dieser UNIX-Pfad im Sicherheitsstil 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
```

Möglichkeiten zum Anzeigen von Informationen über Dateisicherheitsrichtlinien und Audit-Richtlinien

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 über alle Dateien und Verzeichnisse unter dem Pfad angezeigt `/1/` Von SVM vs1:

```
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 Informationen zu einer Datei mit dem Namen „*“ unter dem Pfad angezeigt `/vol1/a` Von SVM vs1. 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 © 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 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.