Sicherer Dateizugriff mit Storage Level Access Guard

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/secure-file-access-storage-level-access-guard-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Sicherer Dateizugriff mit Storage Level Access Guard . . . 1
Informationen zum sicheren ONTAP SMB Dateizugriff mit Storage-Level Access Guard . . . 1
Verhalten des Storage-Level Access Guard . . . 1
Reihenfolge der Zugriffskontrollen . . . 2
Anwendungsfälle für den Einsatz von Storage-Level Access Guard . . . 2
Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB Servern . . . 3
Storage-Level Access Guard auf ONTAP SMB-Servern konfigurieren . . . 5
Effektive SLAG-Matrix auf ONTAP SMB Servern . . . 10
Informationen zu Storage-Level Access Guard auf ONTAP SMB-Servern . . . 11
Storage-Level Access Guard auf ONTAP SMB-Servern entfernen . . . 13

Sicherer Dateizugriff mit Storage Level Access Guard

Informationen zum sicheren ONTAP SMB Dateizugriff mit Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native Dateisicherheits- sowie Export- und Freigabesicherheitsmechanismen kann Storage-Level Access Guard konfiguriert werden, eine dritte Sicherheitsebene, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff aus allen NAS-Protokollen auf das Speicherobjekt, auf das sie angewendet wird.

Es werden ausschließlich NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP Sicherheitsprüfungen für UNIX-Benutzer beim Zugriff auf Daten auf Volumes durchführen kann, für die Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM zugeordnet sein, der das Volume besitzt.

Verhalten des Storage-Level Access Guard

- Storage-Level Access Guard gilt für alle Dateien oder alle Verzeichnisse in einem Storage-Objekt.

  Da alle Dateien oder Verzeichnisse in einem Volume den Einstellungen des Storage-Level Access Guard unterliegen, ist eine Vererbung durch Weitergabe nicht erforderlich.

- Storage-Level Access Guard kann so konfiguriert werden, dass es nur für Dateien, nur für Verzeichnisse oder sowohl für Dateien als auch für Verzeichnisse innerhalb eines Volumes gilt.
  - Datei- und Verzeichnissicherheit

    Gilt für jedes Verzeichnis und jede Datei innerhalb des Speicherobjekts. Dies ist die Standardeinstellung.

  - Dateisicherheit

    Gilt für jede Datei innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Verzeichnissen aus.

  - Verzeichnissicherheit

    Gilt für jedes Verzeichnis innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Dateien aus.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

- Wenn die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus angezeigt werden, ist die Storage-Level Access Guard Sicherheit nicht sichtbar.

  Sie wird auf Ebene des Speicherobjekts angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Die Sicherheit auf Storage-Ebene kann einem Client nicht entzogen werden, auch nicht von einem Systemadministrator (Windows oder UNIX).

  Es ist so konzipiert, dass es nur von Speicheradministratoren geändert werden kann.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS- oder gemischtem Sicherheitsstil anwenden.
- Sie können Storage-Level Access Guard auf Volumes mit UNIX-Sicherheitsstil anwenden, sofern auf der SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume Verbindungspfad gemountet werden und Storage-Level Access Guard auf diesem Pfad vorhanden ist, wird es nicht auf die darunter gemounteten Volumes übertragen.
- Der Storage-Level Access Guard Sicherheitsdeskriptor wird mit SnapMirror Datenreplizierung und mit SVM-Replikation repliziert.
- Für Virenscanner gelten Sonderregelungen.

  Diesen Servern wird ein Ausnahmezugriff zum Durchsuchen von Dateien und Verzeichnissen gewährt, selbst wenn Storage-Level Access Guard den Zugriff auf das Objekt verweigert.

- FPolicy-Benachrichtigungen werden nicht gesendet, wenn der Zugriff aufgrund von Storage-Level Access Guard verweigert wird.

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch die kombinierte Wirkung der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Storage-Level Access Guard-Berechtigungen und der nativ auf Dateien und/oder Verzeichnisse angewendeten Dateiberechtigungen bestimmt. Alle Sicherheitsebenen werden ausgewertet, um zu bestimmen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis hat. Die Sicherheitszugriffsprüfungen erfolgen in folgender Reihenfolge:

1. SMB-Freigabe- oder NFS-Export-Berechtigungen
2. Zugriffsschutz auf Storage-Ebene
3. NTFS-Datei-/Ordnerzugriffskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modusbits

Anwendungsfälle für den Einsatz von Storage-Level Access Guard

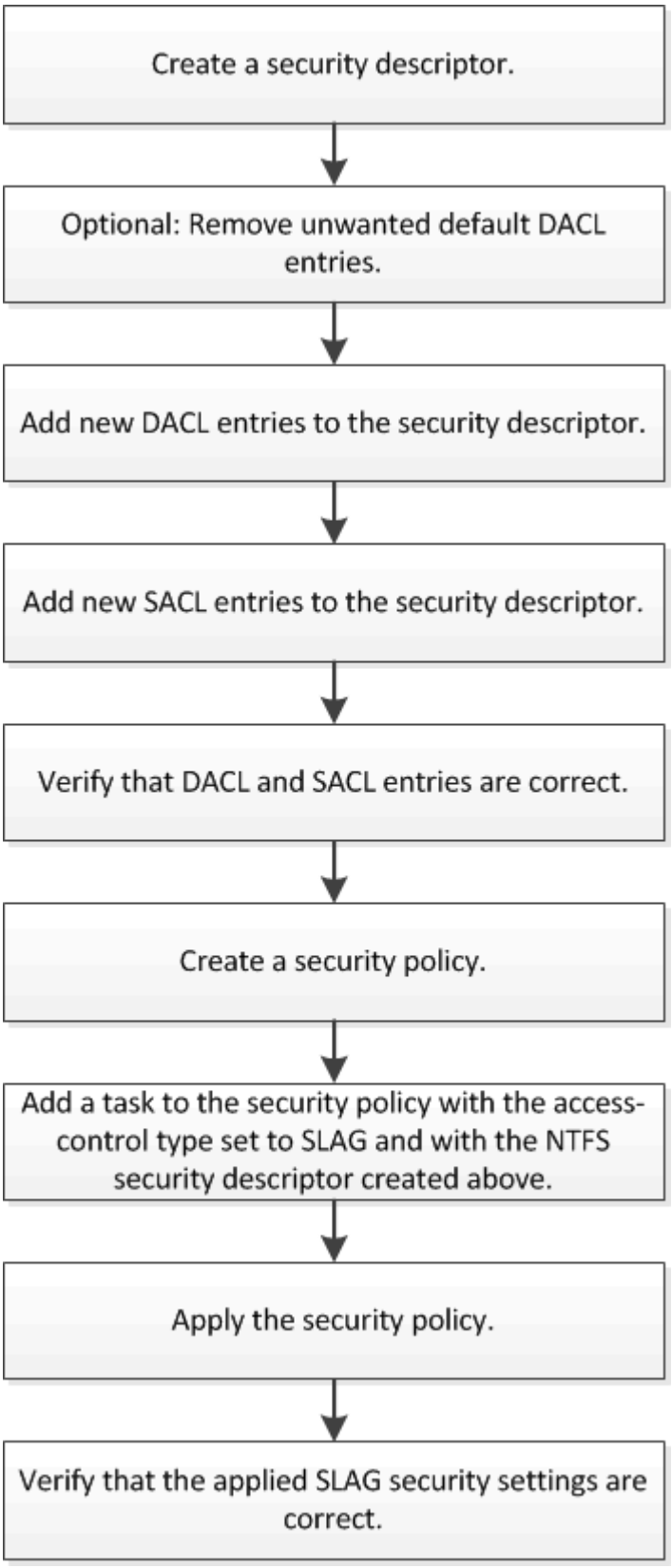
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Speicherebene, die für Clients nicht sichtbar ist, daher kann sie weder von Benutzern noch von Administratoren von ihren Desktops aus aufgehoben werden. In bestimmten Anwendungsfällen ist die Möglichkeit, den Zugriff auf Speicherebene zu steuern, von Vorteil.

Typische Anwendungsfälle für diese Funktion umfassen die folgenden Szenarien:

- Schutz des geistigen Eigentums durch Prüfung und Kontrolle aller Benutzerzugriffe auf Speicherebene
- Storage für Finanzdienstleistungsunternehmen, einschließlich Banken und Handelsgruppen
- Regierungsdienste mit separatem Dateispeicher für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB Servern

Der Workflow zur Konfiguration von Storage-Level Access Guard (SLAG) verwendet dieselben ONTAP CLI-Befehle wie die Konfiguration von NTFS-Dateiberechtigungen und Überwachungsrichtlinien. Statt den Datei- und Verzeichniszugriff auf einem bestimmten Ziel zu konfigurieren, wird SLAG auf dem entsprechenden Volume der Storage Virtual Machine (SVM) konfiguriert.



Verwandte Informationen

Storage Level Access Guard auf Servern konfigurieren

Storage-Level Access Guard auf ONTAP SMB-Servern konfigurieren

Es sind mehrere Schritte erforderlich, um Storage-Level Access Guard auf einem Volume oder Qtree zu konfigurieren. Storage-Level Access Guard bietet eine Zugriffssicherheit, die auf Speicherebene festgelegt wird. Sie bietet eine Sicherheit, die für alle Zugriffe aller NAS-Protokolle auf das Speicherobjekt gilt, auf das sie angewendet wurde.

Schritte

1. Ein Sicherheitsdeskriptor wird mithilfe des `vserver security file-directory ntfs create` Befehls erstellt.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Ein Sicherheitsdeskriptor wird mit den folgenden vier Standard-DACL-Zugriffskontrolleinträgen (ACEs) erstellt:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Wenn Sie bei der Konfiguration von Storage-Level Access Guard nicht die Standardeinträge verwenden möchten, können Sie diese entfernen, bevor Sie eigene ACEs erstellen und dem Sicherheitsdeskriptor hinzufügen.

2. Entfernen Sie alle standardmäßigen DACL-ACEs aus dem Sicherheitsdeskriptor, die nicht mit Storage-Level Access Guard Sicherheit konfiguriert werden sollen:

   a. Unerwünschte DACL-ACEs lassen sich mit dem `vserver security file-directory ntfs dacl remove` Befehl entfernen.

      In diesem Beispiel werden drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt: BUILTIN\Administrators, BUILTIN\Users und CREATOR OWNER.

      ```
      vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
      -access-type allow -account builtin\users vserver security file-directory
      ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
      builtin\administrators vserver security file-directory ntfs dacl remove
      -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
      ```

   b. Es sollte überprüft werden, dass die DACL-ACEs, die nicht für die Storage-Level Access Guard Sicherheit verwendet werden sollen, mithilfe des `vserver security file-directory ntfs dacl show` Befehls aus dem Sicherheitsdeskriptor entfernt wurden.

      In diesem Beispiel bestätigt die Ausgabe des Befehls, dass drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt wurden, sodass nur noch der NT AUTHORITY\SYSTEM Standard-DACL-ACE-Eintrag übrig bleibt:

      ```
      vserver security file-directory ntfs dacl show -vserver vs1
      ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs dacl add` Befehl ein oder mehrere DACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei DACL-ACEs hinzugefügt:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs sacl add` Befehl ein oder mehrere SACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-ACEs hinzugefügt:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Es sollte überprüft werden, ob die DACL- und SACL-ACEs mithilfe der `vserver security file-directory ntfs dacl show`- und `vserver security file-directory ntfs sacl show` -Befehle jeweils korrekt konfiguriert sind.

   In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   In diesem Beispiel zeigt der folgende Befehl Informationen über SACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   ```

```
files
```

6. Eine Sicherheitsrichtlinie kann mithilfe des `vserver security file-directory policy create` Befehls erstellt werden.

   Das folgende Beispiel erstellt eine Richtlinie mit dem Namen “policy1”:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Es kann mithilfe des `vserver security file-directory policy show` Befehls überprüft werden, ob die Richtlinie korrekt konfiguriert ist.

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. Eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor wird zur Sicherheitsrichtlinie hinzugefügt, indem der `vserver security file-directory policy task add` Befehl mit dem `-access -control` Parameter, der auf `slag` gesetzt ist, verwendet wird.

   Eine Richtlinie kann zwar mehrere Storage-Level Access Guard Aufgaben enthalten, jedoch ist es nicht möglich, eine Richtlinie so zu konfigurieren, dass sie sowohl Datei-Verzeichnis- als auch Storage-Level Access Guard Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

   In diesem Beispiel wird der Richtlinie mit dem Namen „policy1“ eine Aufgabe hinzugefügt, die dem Sicherheitsdeskriptor „sd1“ zugewiesen ist. Sie ist dem `/datavol1` Pfad mit dem Zugriffskontrolltyp „slag“ zugeordnet.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Es kann überprüft werden, ob die Aufgabe korrekt konfiguriert ist, indem der `vserver security file-directory policy task show` Befehl verwendet wird.

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
   ```

```
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Die Sicherheitsrichtlinie „Storage-Level Access Guard“ wird mithilfe des `vserver security file-directory apply` Befehls angewendet.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist terminiert.

11. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob die angewendeten Storage-Level Access Guard Sicherheitseinstellungen korrekt sind.

    In diesem Beispiel zeigt die Ausgabe des Befehls, dass die Storage-Level Access Guard-Sicherheit auf das NTFS-Volume angewendet wurde `/datavol1`. Auch wenn die standardmäßige DACL, die Vollzugriff für Everyone erlaubt, weiterhin besteht, beschränkt und protokolliert die Storage-Level Access Guard-Sicherheit den Zugriff auf die in den Storage-Level Access Guard-Einstellungen definierten Gruppen.

    ```
    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

- Befehle zur Verwaltung der NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und des Storage-Level Access Guard
- Konfigurationsworkflow für Storage-Level Access Guard auf Servern
- Informationen zu Storage-Level Access Guard auf Servern
- Storage-Level Access Guard auf Servern entfernen

Effektive SLAG-Matrix auf ONTAP SMB Servern

Sie können SLAG auf einem Volume, einem Qtree oder beiden konfigurieren. Die SLAG-Matrix definiert, auf welchem Volume oder Qtree die SLAG-Konfiguration in den verschiedenen, in der Tabelle aufgeführten Szenarien anwendbar ist.

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	k. A.	k. A.
Volumenzugriff in einer Snapshot	JA	NEIN	k. A.	k. A.
Qtree-Zugriff in einem AFS (wenn SLAG im Qtree vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn SLAG nicht im Qtree vorhanden ist)	JA	NEIN	NEIN	NEIN
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS vorhanden ist)	NEIN	NEIN	JA	NEIN

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS nicht vorhanden ist)	JA	NEIN	NEIN	NEIN

Informationen zu Storage-Level Access Guard auf ONTAP SMB-Servern

Storage-Level Access Guard ist eine dritte Sicherheitsebene, die auf ein Volume oder einen Qtree angewendet wird. Storage-Level Access Guard-Einstellungen können nicht über das Windows-Eigenschaftenfenster angezeigt werden. Zur Anzeige von Informationen zur Storage-Level Access Guard-Sicherheit, die zur Validierung der Konfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden können, ist die ONTAP CLI zu nutzen.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder Qtree angeben, dessen Storage-Level Access Guard Sicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

Schritt

1. Storage-Level Access Guard-Sicherheitseinstellungen 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 Storage-Level Access Guard-Sicherheitsinformationen für das NTFS-Sicherheitsvolume 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
```

Das folgende Beispiel zeigt die Storage-Level Access Guard-Informationen zum Volume mit gemischtem Sicherheitsstil am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Volumes hat 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
                        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
```

Storage-Level Access Guard auf ONTAP SMB-Servern entfernen

Sie können den Storage-Level Access Guard für ein Volume oder einen Qtree entfernen, wenn Sie die Zugriffssicherheit nicht mehr auf Storage-Level festlegen möchten. Das Entfernen des Storage-Level Access Guard ändert oder entfernt die reguläre NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob für das Volume oder den Qtree Storage-Level Access Guard konfiguriert ist.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

   ```
                    Vserver: vs1
                  File Path: /datavol2
          File Inode Number: 99
             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:0xbf14
                        Owner:BUILTIN\Administrators
                        Group:BUILTIN\Administrators
                        SACL - ACEs
                          AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                        DACL - ACEs
                          ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                          ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                        Storage-Level Access Guard security
                        DACL (Applies to Directories):
                          ALLOW-BUILTIN\Administrators-0x1f01ff
                          ALLOW-CREATOR OWNER-0x1f01ff
                          ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                        DACL (Applies to Files):
                          ALLOW-BUILTIN\Administrators-0x1f01ff
                          ALLOW-CREATOR OWNER-0x1f01ff
                          ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Storage-Level Access Guard kann mit dem `vserver security file-directory remove-slag` Befehl entfernt werden.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Es kann mit dem `vserver security file-directory show` Befehl überprüft werden, ob Storage-Level Access Guard vom Volume oder Qtree entfernt wurde.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

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.