



Sicherer Dateizugriff über Storage-Level Access Guard

ONTAP 9

NetApp
January 08, 2026

Inhalt

Sicherer Dateizugriff über Storage-Level Access Guard	1
Erfahren Sie mehr über den sicheren ONTAP SMB-Dateizugriff mithilfe von Storage-Level Access Guard ..	1
Verhalten des Access Guard auf Storage-Ebene	1
Reihenfolge der Zugriffskontrollen	2
Anwendungsfälle für die Verwendung von Storage-Level Access Guard	2
Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB-Servern	3
Konfigurieren Sie Storage-Level Access Guard auf ONTAP SMB-Servern	5
Effektive SLAG-Matrix auf ONTAP SMB-Servern	11
Informationen zum Storage-Level Access Guard auf ONTAP SMB-Servern anzeigen	11
Entfernen Sie Storage-Level Access Guard auf ONTAP SMB-Servern	14

Sicherer Dateizugriff über Storage-Level Access Guard

Erfahren Sie mehr über den sicheren ONTAP SMB-Dateizugriff mithilfe von Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native File-Level und die Sicherheit für Export und Freigabe können Sie den Storage-Level Access Guard konfigurieren, eine dritte Sicherheitsschicht, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff von allen NAS-Protokollen auf das Storage-Objekt, auf das es angewendet wird.

Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.

Verhalten des Access Guard auf Storage-Ebene

- 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 für den Speicherlevel Access Guard unterliegen, ist keine Vererbung durch die Ausbreitung erforderlich.

- Sie können den Storage-Level Access Guard so konfigurieren, dass er nur auf Dateien, nur Verzeichnisse oder auf Dateien und Verzeichnisse innerhalb eines Volumes angewendet wird.
 - Datei- und Verzeichnissicherheit

Gilt für jedes Verzeichnis und jede Datei im Storage-Objekt. Dies ist die Standardeinstellung.

- Dateisicherheit

Gilt für jede Datei im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Verzeichnissen.

- Verzeichnissicherheit

Gilt für jedes Verzeichnis im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Dateien.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

Es wird niemals zusätzliche Zugriffsrechte geben.

- Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Storage-Level Access Guard nicht angezeigt.

Sie wird auf Storage-Objektebene angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Sicherheit auf Storage-Ebene kann nicht durch einen Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt.

Dieses Design lässt sich nur von Storage-Administratoren ändern.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS oder einem gemischten Sicherheitsstil anwenden.
- Sie können Access Guard auf Storage-Ebene auf Volumes mit UNIX-Sicherheitsstil anwenden, solange für die SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume-Verbindungs pfad gemountet werden und wenn Access Guard auf Storage-Ebene auf diesem Pfad vorhanden ist, wird sie nicht auf Volumes übertragen, die darunter angehängt sind.
- Der Sicherheitsdeskriptor für den Storage-Level Access Guard wird mit SnapMirror Datenreplizierung und SVM-Replizierung repliziert.
- Es gibt spezielle Dispensierung für Virenscanner.

Der Zugriff auf diese Server ist auf die Anzeige von Dateien und Verzeichnissen gestattet, selbst wenn der Access Guard auf Storage-Ebene den Zugriff auf das Objekt verweigert.

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

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch den kombinierten Effekt der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Zugriffsschutz auf Storage-Ebene und der nativen Dateiberechtigungen auf Dateien und/oder Verzeichnisse bestimmt. Alle Sicherheitsstufen werden ausgewertet, um festzustellen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis besitzt. Die Sicherheitszugriffskontrollen werden in folgender Reihenfolge durchgeführt:

1. SMB-Freigabe- oder NFS-Berechtigungen für den Export
2. Storage-Level Access Guard
3. NTFS-Datei-/Ordnerzugangskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modus-Bits

Anwendungsfälle für die Verwendung von Storage-Level Access Guard

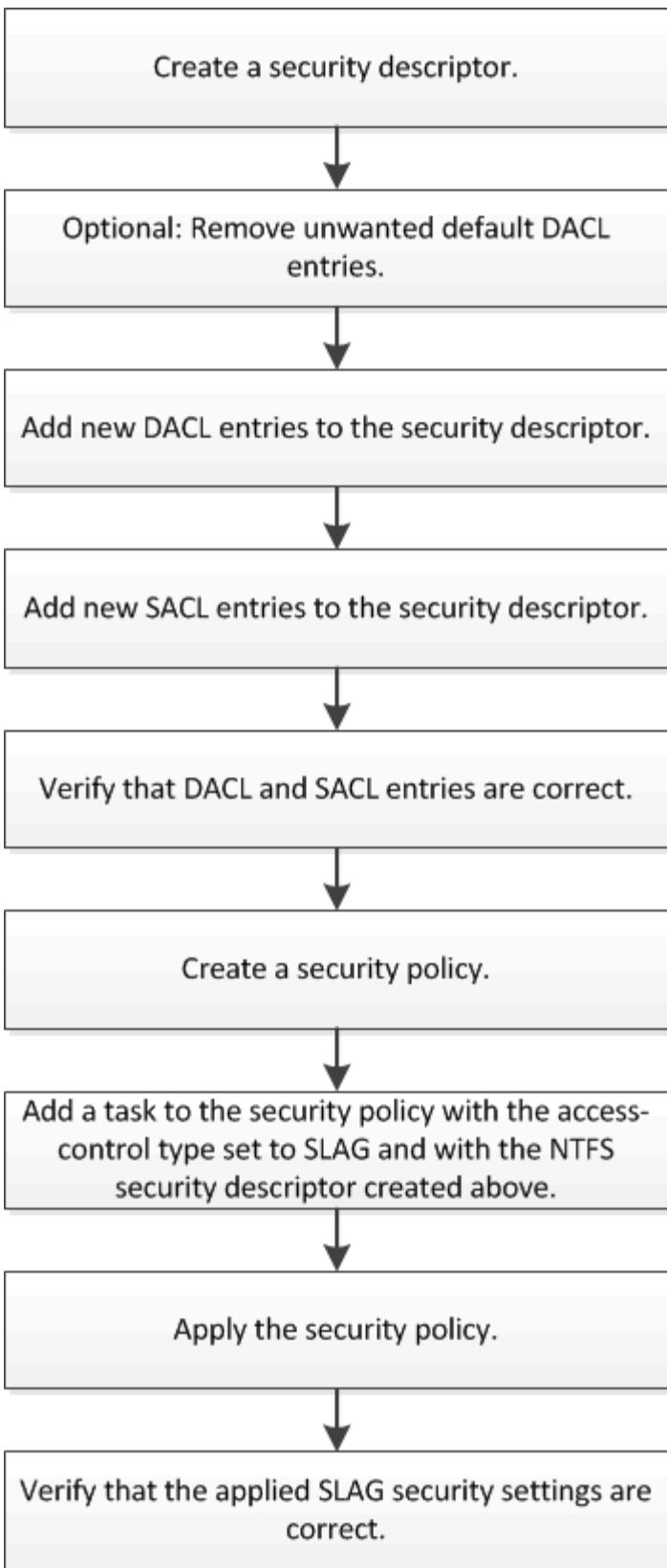
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Storage-Ebene, die nicht von Client-Seite sichtbar ist. Daher kann diese Sicherheit nicht von Benutzern oder Administratoren mit ihren Desktops entzogen werden. In bestimmten Anwendungsfällen ist die Zugriffskontrolle auf Storage-Ebene von Vorteil.

Zu den typischen Anwendungsfällen für diese Funktion zählen folgende Szenarien:

- Schutz geistigen Eigentums durch Auditing und Controlling aller Benutzer` Zugriff auf Storage-Ebene
- Storage für Finanzdienstleister einschließlich Bank- und Handelskonzerne
- Öffentlicher Dienst mit separatem File Storage für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB-Servern

Der Workflow zum Konfigurieren von Storage-Level Access Guard (SCHLACKE) verwendet dieselben ONTAP-CLI-Befehle, mit denen Sie NTFS-Dateiberechtigungen und Audit-Richtlinien konfigurieren. Anstatt Datei- und Verzeichniszugriff auf einem festgelegten Ziel zu konfigurieren, konfigurieren Sie LAG auf dem zugewiesenen SVM-Volume (Storage Virtual Machine).



Verwandte Informationen

[Konfigurieren des Storage-Level Access Guard auf Servern](#)

Konfigurieren Sie Storage-Level Access Guard auf ONTAP SMB-Servern

Zur Konfiguration des Storage-Level Access Guard auf einem Volume oder qtree müssen Sie verschiedene Schritte befolgen. Access Guard auf Storage-Ebene bietet eine Zugriffssicherheit, die auf Storage-Ebene festgelegt ist. Das Tool bietet Sicherheit, die für alle Zugriffe aus allen NAS-Protokollen auf das Storage-Objekt gilt, auf das es angewendet wurde.

Schritte

1. Erstellen Sie mit dem vserver security file-directory ntfs create Befehl einen Sicherheitsdeskriptor.

```
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-Zugriffssteuerungseinträgen (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 die Standardeinträge bei der Konfiguration des Speicher-Level Access Guard nicht verwenden möchten, können Sie sie vor dem Erstellen und Hinzufügen eigener Asse zum Sicherheitsdeskriptor

entfernen.

2. Entfernen Sie eine der Standard-DACL-Aces aus dem Sicherheitsdeskriptor, den Sie nicht mit der Sicherheit für den Speicherlevel Access Guard konfigurieren möchten:
 - a. Entfernen Sie alle unerwünschten ACEs der DACL mit dem `vserver security file-directory ntfs dacl remove` Befehl.

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. Vergewissern Sie sich, dass die DACL-Aces, die Sie nicht für die Sicherheit des Storage-Level Access Guard verwenden möchten `vserver security file-directory ntfs dacl show`, mithilfe des Befehls aus der Sicherheitsbeschreibung entfernt werden.

In diesem Beispiel überprüft die Ausgabe des Befehls, ob drei Standard-DACL-Aces aus dem Sicherheitsdeskriptor entfernt wurden und nur der NT AUTHORITY\SYSTEM Standard-DACL ACE-Eintrag hinterlassen wurde:

```
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. Fügen Sie einen oder mehrere DACL-Einträge zu einem Sicherheitsdeskriptor hinzu `vserver security file-directory ntfs dacl add`, indem Sie den Befehl verwenden.

In diesem Beispiel werden dem Sicherheitsdeskriptor zwei DACL-Asse 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. Fügen Sie einen oder mehrere SACL-Einträge zu einem Sicherheitsdeskriptor hinzu `vserver security file-directory ntfs sacl add`, indem Sie den Befehl verwenden.

In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-Asse 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. Überprüfen Sie mit den vserver security file-directory ntfs dacl show vserver security file-directory ntfs sacl show Befehlen und, ob die ACEs für DACL und SACL korrekt konfiguriert sind.

In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für 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 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. Erstellen Sie mit dem vserver security file-directory policy create Befehl eine Sicherheitsrichtlinie.

Im folgenden Beispiel wird eine Richtlinie mit dem Namen „policy1“ erstellt:

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

7. Überprüfen Sie mit dem vserver security file-directory policy show Befehl, ob die Richtlinie ordnungsgemäß konfiguriert ist.

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

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

8. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugeordneten Sicherheitsdeskriptor hinzu, indem Sie den vserver security file-directory policy task add Befehl mit dem -access-control auf festgelegten Parameter verwenden slag.

Obwohl eine Richtlinie mehr als eine Access Guard-Aufgabe auf Storage-Ebene enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Datei-Verzeichnis- als auch Zugriffsschutz-Aufgaben auf Storage-Ebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

In diesem Beispiel wird der Richtlinie „policy1“ eine Aufgabe hinzugefügt, die dem Sicherheitsdeskriptor „sd1“ zugewiesen ist. Er wird dem /datavoll Pfad zugewiesen, wobei der Zugriffskontrolltyp auf „slag“ gesetzt ist.

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

9. Überprüfen Sie mit dem vserver security file-directory policy task show Befehl, ob die

Aufgabe ordnungsgemäß konfiguriert ist.

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

Vserver:	vs1			
Policy:	policy1			
Index	File/Folder	Access	Security	NTFS
Security	Path	Control	Type	Mode
Name				Descriptor
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
1	/datavol1	slag	ntfs	propagate sd1

10. Wenden Sie die Sicherheitsrichtlinie `vserver security file-directory apply` für den Access Guard auf Specherebene mit dem Befehl an.

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

Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist geplant.

11. Überprüfen Sie mit dem `vserver security file-directory show` Befehl, ob die Sicherheitseinstellungen des Access Guard auf Specherebene korrekt sind.

In diesem Beispiel zeigt die Ausgabe des Befehls, dass die Sicherheit des Access Guard auf Specherebene auf das NTFS-Volume angewendet wurde /datavol1. Obwohl die Standard-DACL, die die volle Kontrolle für alle zulässt, bleibt, schränkt die Sicherheit auf Storage-Ebene den Zugriff auf die in den Einstellungen für den Speicher-Level Access Guard definierten Gruppen ein (und prüft).

```
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 zum Verwalten der NTFS-Dateisicherheit, der NTFS-Überwachungsrichtlinien und des Storage-Level Access Guard
- Konfigurationsworkflow für Storage-Level Access Guard auf Servern
- Informationen zum Storage-Level Access Guard auf Servern anzeigen
- Entfernen Sie Storage-Level Access Guard auf Servern

Effektive SLAG-Matrix auf ONTAP SMB-Servern

SIE können LAG auf einem Volume oder einem qtree oder beiden konfigurieren. Die SCHLACKE-Matrix definiert, auf welchem Volume oder qtree die SCHLACKE-Konfiguration ist. Sie wird unter verschiedenen in der Tabelle aufgeführten Szenarien angewendet.

	Volumen-SCHLACKE in einem AFS	Volume-LAG in einem Snapshot	Qtree SCHLACKE in einem AFS	Qtree SCHLACKE in einem Snapshot
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	1. A.	1. A.
Volume-Zugriff in einem Snapshot	JA	NEIN	1. A.	1. A.
Qtree-Zugriff in einem AFS (wenn IM qtree SCHLACKE vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn LAG 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
Qtree-Zugriff in einem Snapshot (wenn SLAG nicht im qtree AFS vorhanden ist)	JA	NEIN	NEIN	NEIN

Informationen zum Storage-Level Access Guard auf ONTAP SMB-Servern anzeigen

Storage-Level Access Guard ist eine dritte Sicherheitsschicht, die auf einem Volume oder qtree angewendet wird. Die Einstellungen für den Zugriffsenschutz auf Speicherebene können nicht über das Fenster „Windows-Eigenschaften“ angezeigt werden. Sie müssen die ONTAP-CLI verwenden, um Informationen zur Sicherheit des Zugriffschutzes auf

Storage-Ebene anzuzeigen, mit der Sie die Konfiguration validieren oder Probleme beim Dateizugriff beheben können.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder qtree angeben, dessen Sicherheitsinformationen auf Storage-Level Access Guard angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

Schritt

1. Die Sicherheitseinstellungen der Speicherebene für den Access Guard mit der gewünschten Detailebene anzeigen:

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

Beispiele

Im folgenden Beispiel werden Sicherheitsinformationen für den Access Guard auf Speicherebene für das NTFS-Sicherheitsvolume mit dem Pfad /datavol1 in SVM vs1 angezeigt:

```

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

```

Im folgenden Beispiel werden die Access Guard-Informationen auf Storage-Ebene über das Volume im gemischten Sicherheitstil im Pfad /datavol5 in SVM vs1 angezeigt. Die oberste Ebene dieses Volumens besitzt effektive UNIX-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
          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

```

Entfernen Sie Storage-Level Access Guard auf ONTAP SMB-Servern

Sie können Storage-Level Access Guard auf einem Volume oder qtree entfernen, wenn Sie nicht mehr die Zugriffssicherheit auf Storage-Ebene festlegen möchten. Das Entfernen von Speicherebene Access Guard ändert oder entfernt die normale NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Mit dem `vserver security file-directory show` Befehl überprüfen Sie, ob für das Volume oder den qtree der 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:0xbff14
            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. Entfernen Sie Access Guard auf Storage-Ebene mit dem vserver security file-directory remove-slag Befehl.

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

3. Überprüfen Sie mit dem vserver security file-directory show Befehl, ob Access Guard auf Storage-Ebene 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:0xbff14
    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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERWEINER 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.