



# **Proteggere l'accesso ai file utilizzando Storage-Level Access Guard**

## **ONTAP 9**

NetApp  
February 12, 2026

# Sommario

Proteggere l'accesso ai file utilizzando Storage-Level Access Guard . . . . .	1
Scopri come accedere in modo sicuro ai file SMB ONTAP utilizzando Storage-Level Access Guard . . . . .	1
Comportamento di Access Guard a livello di storage . . . . .	1
Ordine dei controlli di accesso . . . . .	2
Casi di utilizzo di Storage-Level Access Guard . . . . .	2
Flusso di lavoro di configurazione per Storage-Level Access Guard sui server ONTAP SMB . . . . .	3
Configurare Storage-Level Access Guard sui server ONTAP SMB . . . . .	5
Matrice SLAG efficace sui server ONTAP SMB . . . . .	11
Visualizza informazioni su Storage-Level Access Guard sui server ONTAP SMB . . . . .	11
Rimuovere Storage-Level Access Guard sui server ONTAP SMB . . . . .	14

# Proteggere l'accesso ai file utilizzando Storage-Level Access Guard

## Scopri come accedere in modo sicuro ai file SMB ONTAP utilizzando Storage-Level Access Guard

Oltre a proteggere l'accesso utilizzando la sicurezza nativa a livello di file e di esportazione e condivisione, è possibile configurare la protezione dell'accesso a livello di storage, un terzo livello di sicurezza applicato da ONTAP a livello di volume. Storage-Level Access Guard si applica all'accesso da tutti i protocolli NAS all'oggetto di storage a cui è applicato.

Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.

### Comportamento di Access Guard a livello di storage

- Storage-Level Access Guard si applica a tutti i file o a tutte le directory di un oggetto di storage.

Poiché tutti i file o le directory di un volume sono soggetti alle impostazioni di Storage-Level Access Guard, non è richiesta l'ereditarietà attraverso la propagazione.

- È possibile configurare Storage-Level Access Guard in modo che si applichi solo ai file, solo alle directory o sia ai file che alle directory all'interno di un volume.
  - Sicurezza di file e directory

Si applica a ogni directory e file all'interno dell'oggetto di storage. Questa è l'impostazione predefinita.

- Sicurezza del file

Si applica a tutti i file all'interno dell'oggetto di storage. L'applicazione di questa protezione non influisce sull'accesso o sul controllo delle directory.

- Sicurezza della directory

Si applica a ogni directory all'interno dell'oggetto di storage. L'applicazione di questa protezione non influisce sull'accesso o sul controllo dei file.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

Non assegnerà mai autorizzazioni di accesso aggiuntive.

- Se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, la protezione Storage-Level Access Guard non viene visualizzata.

Viene applicato a livello di oggetto di storage e memorizzato nei metadati utilizzati per determinare le autorizzazioni effettive.

- La sicurezza a livello di storage non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX).

È progettato per essere modificato solo dagli amministratori dello storage.

- È possibile applicare Storage-Level Access Guard a volumi con NTFS o stile di sicurezza misto.
- È possibile applicare Storage-Level Access Guard ai volumi con lo stile di sicurezza UNIX, purché la SVM contenente il volume abbia configurato un server CIFS.
- Quando i volumi sono montati sotto un percorso di giunzione del volume e se Storage-Level Access Guard è presente su tale percorso, non verrà propagata ai volumi montati sotto di esso.
- Il descrittore di sicurezza Storage-Level Access Guard viene replicato con la replica dei dati SnapMirror e con la replica SVM.
- Esiste una dispensazione speciale per i virus scanner.

A questi server è consentito un accesso eccezionale per lo screening di file e directory, anche se Storage-Level Access Guard nega l'accesso all'oggetto.

- Le notifiche FPolicy non vengono inviate se l'accesso viene negato a causa di Storage-Level Access Guard.

## Ordine dei controlli di accesso

L'accesso a un file o a una directory è determinato dall'effetto combinato delle autorizzazioni di esportazione o condivisione, delle autorizzazioni Storage-Level Access Guard impostate sui volumi e delle autorizzazioni native dei file applicate a file e/o directory. Tutti i livelli di sicurezza vengono valutati per determinare le autorizzazioni effettive di un file o di una directory. I controlli di accesso di sicurezza vengono eseguiti nel seguente ordine:

1. Permessi di condivisione SMB o NFS a livello di esportazione
2. Access Guard a livello di storage
3. ACL (Access Control List) file/cartelle NTFS, ACL NFSv4 o bit di modalità UNIX

## Casi di utilizzo di Storage-Level Access Guard

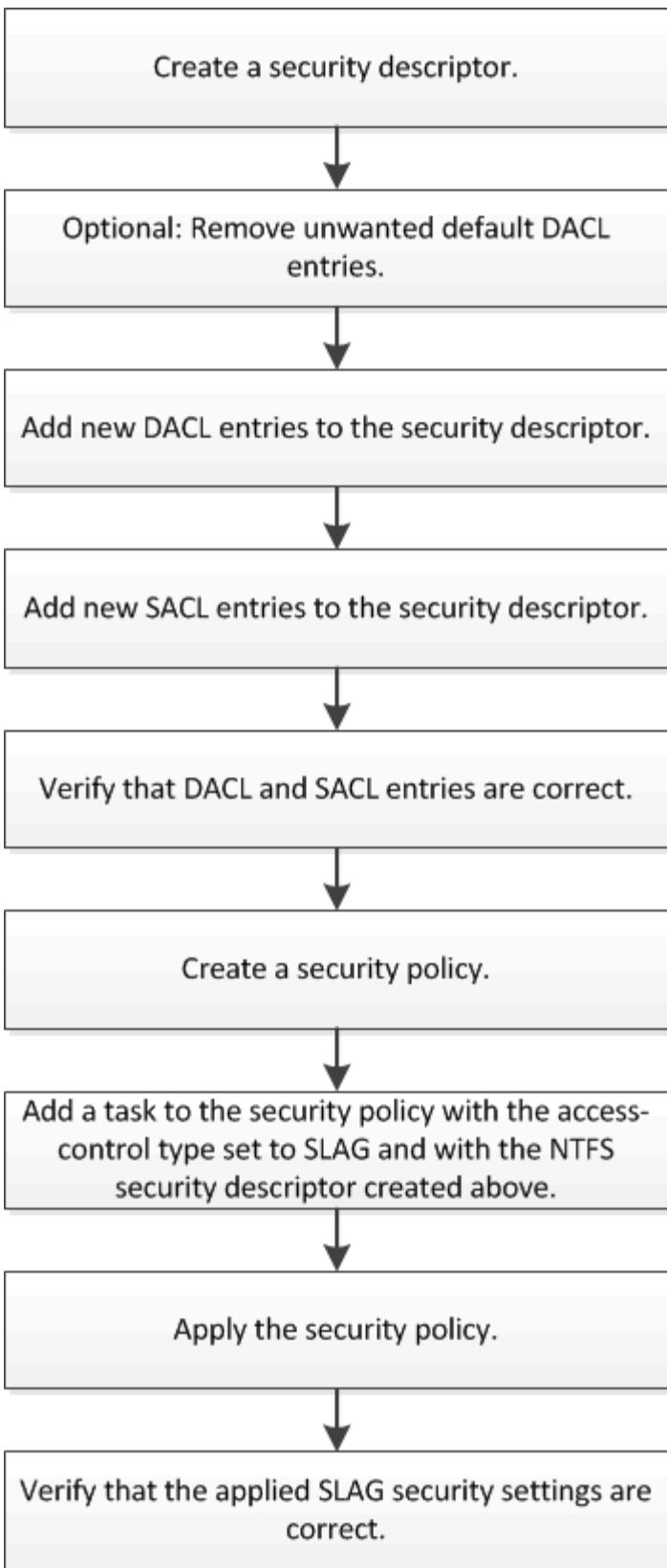
Storage-Level Access Guard offre una sicurezza aggiuntiva a livello di storage, che non è visibile dal lato client; pertanto, non può essere revocata da nessuno degli utenti o degli amministratori dai propri desktop. Esistono alcuni casi di utilizzo in cui la capacità di controllare l'accesso a livello di storage è vantaggiosa.

I casi di utilizzo tipici di questa funzionalità includono i seguenti scenari:

- Protezione della proprietà intellettuale attraverso il controllo e il controllo dell'accesso di tutti gli utenti a livello di storage
- Storage per le società di servizi finanziari, inclusi gruppi bancari e commerciali
- Servizi governativi con storage di file separato per singoli reparti
- Le università proteggono tutti i file degli studenti

## **Flusso di lavoro di configurazione per Storage-Level Access Guard sui server ONTAP SMB**

Il flusso di lavoro per la configurazione di Storage-Level Access Guard (SLAG) utilizza gli stessi comandi CLI di ONTAP utilizzati per configurare le autorizzazioni dei file NTFS e i criteri di controllo. Invece di configurare l'accesso a file e directory su una destinazione designata, è possibile configurare LO SLAG sul volume SVM (Storage Virtual Machine) designato.



#### Informazioni correlate

[Configurare Storage-Livello Access Guard sui server](#)

# Configurare Storage-Level Access Guard sui server ONTAP SMB

Per configurare Storage-Level Access Guard su un volume o su un qtree, è necessario seguire una serie di passaggi. Storage-Level Access Guard offre un livello di sicurezza degli accessi impostato a livello di storage. Fornisce una sicurezza che si applica a tutti gli accessi da tutti i protocolli NAS all'oggetto di storage a cui è stato applicato.

## Fasi

1. Creare un descrittore di protezione utilizzando vserver security file-directory ntfs create comando.

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

```
Vserver: vs1
```

NTFS Security Descriptor Name	Owner Name
sd1	-

Viene creato un descrittore di protezione con le seguenti quattro voci di controllo di accesso DACL predefinite:

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
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

Se non si desidera utilizzare le voci predefinite durante la configurazione di Storage-Level Access Guard, è possibile rimuoverle prima di creare e aggiungere le proprie ACE al descrittore di protezione.

2. Rimuovere dal descrittore di protezione una delle ACL DACL predefinite che non si desidera configurare con la protezione Storage-Level Access Guard:

a. Rimuovere eventuali ACL DACL indesiderati utilizzando vserver security file-directory ntfs dacl remove comando.

In questo esempio, tre ACL DACL predefiniti vengono rimossi dal descrittore di protezione: BUILTIN/Administrators, BUILTIN/Users e 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. Verificare che le ACL DACL che non si desidera utilizzare per la protezione Storage-Level Access Guard siano rimosse dal descrittore di protezione utilizzando vserver security file-directory ntfs dacl show comando.

In questo esempio, l'output del comando verifica che tre ACL DACL predefinite siano state rimosse dal descrittore di protezione, lasciando solo la voce ACE DACL predefinita di sistema/AUTORITÀ NT:

```
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. Aggiungere una o più voci DACL a un descrittore di protezione utilizzando vserver security file-directory ntfs dacl add comando.

In questo esempio, due ACL DACL vengono aggiunti al descrittore di protezione:

```
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. Aggiungere una o più voci SACL a un descrittore di protezione utilizzando vserver security file-directory ntfs sacl add comando.

In questo esempio, due ACL SACL vengono aggiunti al descrittore di protezione:

```
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. Verificare che le ACL DACL e SACL siano configurate correttamente utilizzando vserver security file-directory ntfs dacl show e. vserver security file-directory ntfs sacl show comandi, rispettivamente.

In questo esempio, il comando seguente visualizza informazioni sulle voci DACL per il descrittore di protezione "sd1":

```
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 questo esempio, il comando seguente visualizza informazioni sulle voci SACL per il descrittore di protezione "sd1":

```
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. Creare un criterio di protezione utilizzando `vserver security file-directory policy create` comando.

Nell'esempio seguente viene creata una policy denominata "policy1":

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

7. Verificare che il criterio sia configurato correttamente utilizzando `vserver security file-directory policy show` comando.

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

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

8. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione utilizzando `vserver security file-directory policy task add` con il `-access-control` parametro impostato su `slag`.

Anche se un criterio può contenere più di un'attività Storage-Level Access Guard, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

In questo esempio, viene aggiunto un task alla policy denominata "policy1", assegnata al descrittore di sicurezza "sd1". Viene assegnato a. /datavol1 percorso con il tipo di controllo dell'accesso impostato su "slag".

```
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. Verificare che l'attività sia configurata correttamente utilizzando `vserver security file-directory policy task show` comando.

```
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	sdl	

10. Applicare il criterio di protezione Storage-Level Access Guard utilizzando `vserver security file-directory apply` comando.

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

Il processo di applicazione della policy di sicurezza è pianificato.

11. Verificare che le impostazioni di protezione di Storage-Level Access Guard applicate siano corrette utilizzando `vserver security file-directory show` comando.

In questo esempio, l'output del comando indica che la protezione Storage-Level Access Guard è stata applicata al volume NTFS /datavol1. Anche se il DACL predefinito che consente il controllo completo a tutti rimane, la protezione di Storage-Level Access Guard limita (e controlla) l'accesso ai gruppi definiti nelle impostazioni di Storage-Level Access Guard.

```
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

```

## Informazioni correlate

- Comandi per la gestione della sicurezza dei file NTFS, dei criteri di controllo NTFS e di Storage-Level Access Guard
- Flusso di lavoro di configurazione per Storage-Level Access Guard sui server
- Visualizza informazioni su Storage-Level Access Guard sui server
- Rimuovere Storage-Livello Access Guard sui server

## Matrice SLAG efficace sui server ONTAP SMB

È possibile configurare LO SLAG su un volume, un qtree o entrambi. La matrice DELLE SCORIE definisce su quale volume o qtree è la configurazione DELLE SCORIE applicabile in diversi scenari elencati nella tabella.

	SCORIA di volume in un AFS	SCHIAVITÙ di volumi in uno snapshot	SCORIE del qtree in un AFS	SCHIAVITÙ DEI qtree in una snapshot
Accesso al volume in un file system di accesso (AFS)	Sì	NO	N/A.	N/A.
Accesso ai volumi in uno snapshot	Sì	NO	N/A.	N/A.
Accesso al qtree in un AFS (quando LA SCORIA è presente nel qtree)	NO	NO	Sì	NO
Accesso al qtree in un AFS (quando LA SCORIA non è presente in qtree)	Sì	NO	NO	NO
Accesso al qtree in una snapshot (quando è presente una SCORIA nel sistema AFS del qtree)	NO	NO	Sì	NO
Accesso al qtree in una snapshot (quando la SCORIA non è presente nell'AFS del qtree)	Sì	NO	NO	NO

## Visualizza informazioni su Storage-Level Access Guard sui server ONTAP SMB

Storage-Level Access Guard è un terzo livello di sicurezza applicato a un volume o qtree. Le impostazioni di Storage-Level Access Guard non possono essere visualizzate utilizzando la finestra Proprietà di Windows. È necessario utilizzare l'interfaccia utente di ONTAP per visualizzare informazioni sulla protezione di Access Guard a livello di storage, che è possibile utilizzare per convalidare la configurazione o risolvere i problemi

di accesso ai file.

#### A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso del volume o del qtree di cui si desidera visualizzare le informazioni di protezione Storage-Level Access Guard. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

#### Fase

1. Visualizzare le impostazioni di sicurezza di Storage-Level Access Guard con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Con dettagli più dettagliati	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

#### Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni di protezione di Storage-Level Access Guard per il volume di sicurezza NTFS con il percorso /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

```

Nell'esempio seguente vengono visualizzate le informazioni di Storage-Level Access Guard relative al volume misto di sicurezza nel percorso /datavol5 In SVM vs1. Il livello superiore di questo volume offre una protezione efficace per UNIX. Il volume dispone della protezione di Storage-Level 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

```

## Rimuovere Storage-Level Access Guard sui server ONTAP SMB

È possibile rimuovere Storage-Level Access Guard su un volume o qtree se non si desidera più impostare la sicurezza dell'accesso a livello di storage. La rimozione di Storage-Level Access Guard non modifica o rimuove la normale protezione di file e directory NTFS.

### Fasi

1. Verificare che nel volume o nel qtree sia configurato Storage-Level Access Guard utilizzando `vserver security file-directory show` comando.

```
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. Rimuovere Storage-Level Access Guard utilizzando vserver security file-directory remove-slag comando.

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

3. Verificare che Storage-Level Access Guard sia stato rimosso dal volume o dal qtree utilizzando vserver security file-directory show comando.

```
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
```

## **Informazioni sul copyright**

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

**LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE:** l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## **Informazioni sul marchio commerciale**

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.