Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per i dati di sicurezza UNIX

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/smb-admin/manage-file-security-clients-unix-style-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per i dati di sicurezza UNIX 1
Scoprite come presentare la sicurezza dei file ONTAP ai client SMB per i dati di sicurezza UNIX 1
Configurare la presentazione degli ACL NTFS ai client SMB di ONTAP per i dati sullo stile di protezione UNIX 2
Informazioni sulla conservazione delle autorizzazioni UNIX per i volumi FlexVol SMB di ONTAP 2
Informazioni sulla gestione delle autorizzazioni UNIX mediante la scheda protezione di Windows per i server SMB ONTAP 2

Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per i dati di sicurezza UNIX

Scoprite come presentare la sicurezza dei file ONTAP ai client SMB per i dati di sicurezza UNIX

Puoi scegliere come presentare la sicurezza dei file ai client SMB per i dati di sicurezza UNIX attivando o disattivando la presentazione degli ACL NTFS ai client SMB. Ogni impostazione offre vantaggi che è necessario comprendere per scegliere l'impostazione più adatta alle proprie esigenze di business.

Per impostazione predefinita, ONTAP presenta le autorizzazioni UNIX sui volumi UNIX di tipo Security ai client SMB come ACL NTFS. Esistono scenari in cui ciò è auspicabile, tra cui:

- Per visualizzare e modificare le autorizzazioni UNIX, utilizzare la scheda **Security** nella casella Proprietà di Windows.

  Non è possibile modificare le autorizzazioni da un client Windows se l'operazione non è consentita dal sistema UNIX. Ad esempio, non è possibile modificare la proprietà di un file non proprietario, perché il sistema UNIX non consente questa operazione. Questa restrizione impedisce ai client SMB di ignorare le autorizzazioni UNIX impostate sui file e sulle cartelle.

- Gli utenti stanno modificando e salvando i file sul volume UNIX di sicurezza utilizzando alcune applicazioni Windows, ad esempio Microsoft Office, in cui ONTAP deve conservare le autorizzazioni UNIX durante le operazioni di salvataggio.
- Nell'ambiente sono presenti alcune applicazioni Windows che prevedono di leggere gli ACL NTFS sui file utilizzati.

In alcuni casi, è possibile disattivare la presentazione delle autorizzazioni UNIX come ACL NTFS. Se questa funzionalità è disattivata, ONTAP presenta i volumi UNIX di sicurezza come volumi FAT ai client SMB. Esistono motivi specifici per cui potresti voler presentare i volumi UNIX di sicurezza come volumi FAT ai client SMB:

- È possibile modificare le autorizzazioni UNIX solo utilizzando i mount sui client UNIX.

  La scheda Security (sicurezza) non è disponibile quando un volume UNIX di tipo Security viene mappato su un client SMB. L'unità mappata sembra essere formattata con il file system FAT, che non dispone di permessi per i file.

- Si stanno utilizzando applicazioni su SMB che impostano ACL NTFS su file e cartelle a cui si accede, il che può verificarsi se i dati risiedono su volumi UNIX di sicurezza.

  Se ONTAP riporta il volume come FAT, l'applicazione non tenta di modificare un ACL.

Informazioni correlate

- Configurare gli stili di sicurezza sui volumi FlexVol
- Configurare gli stili di sicurezza sui qtree

Configurare la presentazione degli ACL NTFS ai client SMB di ONTAP per i dati sullo stile di protezione UNIX

È possibile attivare o disattivare la presentazione degli ACL NTFS ai client SMB per i dati di sicurezza UNIX (volumi di sicurezza UNIX e volumi di sicurezza misti con protezione efficace UNIX).

A proposito di questa attività

Se si attiva questa opzione, ONTAP presenta file e cartelle su volumi con uno stile di sicurezza UNIX efficace ai client SMB come dotati di ACL NTFS. Se si disattiva questa opzione, i volumi vengono presentati come volumi FAT ai client SMB. L'impostazione predefinita prevede la presentazione degli ACL NTFS ai client SMB.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'impostazione dell'opzione UNIX NTFS ACL: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -vserver` *`vserver_name`*
4. Tornare al livello di privilegio admin: `set -privilege admin`

Informazioni sulla conservazione delle autorizzazioni UNIX per i volumi FlexVol SMB di ONTAP

Quando i file in un volume FlexVol che dispongono attualmente di autorizzazioni UNIX vengono modificati e salvati dalle applicazioni Windows, ONTAP può conservare le autorizzazioni UNIX.

Quando le applicazioni sui client Windows modificano e salvano i file, leggono le proprietà di protezione del file, creano un nuovo file temporaneo, applicano tali proprietà al file temporaneo e assegnano al file temporaneo il nome del file originale.

Quando i client Windows eseguono una query per le proprietà di protezione, ricevono un ACL costruito che rappresenta esattamente le autorizzazioni UNIX. L'unico scopo di questo ACL costruito è quello di preservare le autorizzazioni UNIX del file, poiché i file vengono aggiornati dalle applicazioni Windows per garantire che i file risultanti abbiano le stesse autorizzazioni UNIX. ONTAP non imposta alcun ACL NTFS utilizzando l'ACL costruito.

Informazioni sulla gestione delle autorizzazioni UNIX mediante la scheda protezione di Windows per i server SMB ONTAP

Se si desidera modificare le autorizzazioni UNIX di file o cartelle in volumi misti di sicurezza o qtree su SVM, è possibile utilizzare la scheda Security (protezione) sui client Windows. In alternativa, è possibile utilizzare applicazioni in grado di eseguire query e impostare gli ACL di Windows.

- Modifica delle autorizzazioni UNIX

  È possibile utilizzare la scheda protezione di Windows per visualizzare e modificare le autorizzazioni UNIX per un volume misto di sicurezza o qtree. Se si utilizza la scheda principale di Windows Security per modificare le autorizzazioni UNIX, è necessario rimuovere prima l'ACE esistente che si desidera modificare (in questo modo i bit di modalità vengono impostati su 0) prima di apportare le modifiche. In alternativa, è possibile utilizzare l'editor avanzato per modificare le autorizzazioni.

  Se vengono utilizzate le autorizzazioni di modalità, è possibile modificare direttamente le autorizzazioni di modalità per UID, GID e altri (tutti gli altri utenti con un account sul computer). Ad esempio, se l'UID visualizzato dispone delle autorizzazioni r-x, è possibile modificare le autorizzazioni UID in rwx.

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

  È possibile utilizzare la scheda protezione di Windows per sostituire gli oggetti di protezione UNIX con oggetti di protezione di Windows su un volume misto di tipo sicurezza o qtree in cui i file e le cartelle hanno uno stile di protezione efficace UNIX.

  Prima di poter sostituire le voci di autorizzazione UNIX con gli oggetti utente e gruppo di Windows desiderati, è necessario rimuovere tutte le voci di autorizzazione UNIX elencate. È quindi possibile configurare gli ACL basati su NTFS sugli oggetti utente e Gruppo di Windows. Rimuovendo tutti gli oggetti di protezione UNIX e aggiungendo solo utenti e gruppi Windows a un file o a una cartella in un volume o qtree misto di sicurezza, è possibile modificare lo stile di protezione effettivo del file o della cartella da UNIX a NTFS.

  Quando si modificano le autorizzazioni di una cartella, il comportamento predefinito di Windows consiste nel propagare queste modifiche a tutte le sottocartelle e a tutti i file. Pertanto, se non si desidera propagare una modifica dello stile di protezione a tutte le cartelle figlio, le sottocartelle e i file, è necessario modificare l'impostazione di propagazione desiderata.

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.