



Utilizzare le opzioni per personalizzare i server SMB

ONTAP 9

NetApp

February 12, 2026

Sommario

Utilizzare le opzioni per personalizzare i server SMB	1
Opzioni server ONTAP per PMI disponibili	1
Configurare le opzioni del server SMB in ONTAP	5
Configurare l'autorizzazione del gruppo UNIX per gli utenti SMB di ONTAP	6
Configurare le restrizioni di accesso SMB a ONTAP per utenti anonimi	6
Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per i dati di sicurezza UNIX	7
Scoprite come presentare la sicurezza dei file ONTAP ai client SMB per i dati di sicurezza UNIX	7
Configurare la presentazione degli ACL NTFS ai client SMB di ONTAP per i dati sullo stile di protezione UNIX	8
Informazioni sulla conservazione delle autorizzazioni UNIX per i volumi FlexVol SMB di ONTAP	8
Informazioni sulla gestione delle autorizzazioni UNIX mediante la scheda protezione di Windows per i server SMB ONTAP	9

Utilizzare le opzioni per personalizzare i server SMB

Opzioni server ONTAP per PMI disponibili

È utile sapere quali opzioni sono disponibili quando si considera come personalizzare il server SMB. Anche se alcune opzioni sono per uso generale sul server SMB, molte vengono utilizzate per abilitare e configurare funzionalità SMB specifiche. Le opzioni dei server SMB sono controllate con `vserver cifs options modify` opzione.

L'elenco seguente specifica le opzioni del server SMB disponibili a livello di privilegi di amministratore:

- **Configurazione del valore di timeout della sessione SMB**

La configurazione di questa opzione consente di specificare il numero di secondi di inattività prima della disconnessione di una sessione SMB. Una sessione inattiva è una sessione in cui un utente non ha file o directory aperti sul client. Il valore predefinito è 900 secondi.

- **Configurazione dell'utente UNIX predefinito**

La configurazione di questa opzione consente di specificare l'utente UNIX predefinito utilizzato dal server SMB. ONTAP crea automaticamente un utente predefinito denominato "pcuser" (con un UID di 65534), crea un gruppo denominato "pcuser" (con un GID di 65534) e aggiunge l'utente predefinito al gruppo "pcuser". Quando si crea un server SMB, ONTAP configura automaticamente "pcuser" come utente UNIX predefinito.

- **Configurazione dell'utente UNIX guest**

La configurazione di questa opzione consente di specificare il nome di un utente UNIX a cui vengono mappati gli utenti che accedono da domini non attendibili, consentendo a un utente di un dominio non attendibile di connettersi al server SMB. Per impostazione predefinita, questa opzione non è configurata (non esiste alcun valore predefinito); pertanto, l'impostazione predefinita è di non consentire agli utenti di domini non attendibili di connettersi al server SMB.

- **Abilitazione o disabilitazione dell'esecuzione della concessione in lettura per i bit di modalità**

L'attivazione o la disattivazione di questa opzione consente di specificare se consentire ai client SMB di eseguire file eseguibili con bit in modalità UNIX ai quali hanno accesso in lettura, anche quando il bit eseguibile UNIX non è impostato. Questa opzione è disattivata per impostazione predefinita.

- **Abilitazione o disabilitazione della possibilità di eliminare i file di sola lettura dai client NFS**

L'attivazione o la disattivazione di questa opzione determina se consentire ai client NFS di eliminare file o cartelle con il set di attributi di sola lettura. La semantica di eliminazione NTFS non consente l'eliminazione di un file o di una cartella quando viene impostato l'attributo di sola lettura. La semantica di eliminazione di UNIX ignora il bit di sola lettura, utilizzando invece le autorizzazioni della directory principale per determinare se un file o una cartella può essere eliminata. L'impostazione predefinita è `disabled`, Che determina la semantica di eliminazione di NTFS.

- **Configurazione degli indirizzi del server Windows Internet Name Service**

La configurazione di questa opzione consente di specificare un elenco di indirizzi del server WINS

(Windows Internet Name Service) come elenco delimitato da virgole. Specificare gli indirizzi IPv4. Gli indirizzi IPv6 non sono supportati. Non esiste alcun valore predefinito.

L'elenco seguente specifica le opzioni del server SMB disponibili al livello di privilegio avanzato:

- **Concessione delle autorizzazioni di gruppo UNIX agli utenti CIFS**

La configurazione di questa opzione determina se all'utente CIFS in entrata che non è il proprietario del file può essere concessa l'autorizzazione di gruppo. Se l'utente CIFS non è il proprietario del file di sicurezza UNIX e questo parametro è impostato su `true`, quindi viene concessa l'autorizzazione di gruppo per il file. Se l'utente CIFS non è il proprietario del file di sicurezza UNIX e questo parametro è impostato su `false`, quindi, le normali regole UNIX sono applicabili per concedere l'autorizzazione al file. Questo parametro è applicabile ai file di sicurezza UNIX con autorizzazione impostata su `mode bits E` non è applicabile ai file con la modalità di sicurezza NTFS o NFSv4. L'impostazione predefinita è `false`.

- **Abilitazione o disabilitazione di SMB 1.0**

SMB 1.0 è disattivato per impostazione predefinita su una SVM per la quale viene creato un server SMB in ONTAP 9.3.



A partire da ONTAP 9.3, SMB 1.0 è disattivato per impostazione predefinita per i nuovi server SMB creati in ONTAP 9.3. È necessario migrare a una versione SMB più recente il prima possibile per prepararsi ai miglioramenti di sicurezza e conformità. Per ulteriori informazioni, contatta il tuo rappresentante NetApp.

- **Abilitazione o disabilitazione di SMB 2.x**

SMB 2.0 è la versione SMB minima che supporta il failover LIF. Se si disattiva SMB 2.x, anche ONTAP disattiva automaticamente SMB 3.X.

SMB 2.0 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione di SMB 3.0**

SMB 3.0 è la versione SMB minima che supporta le condivisioni a disponibilità continua. Windows Server 2012 e Windows 8 sono le versioni minime di Windows che supportano SMB 3.0.

SMB 3.0 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione di SMB 3.1**

Windows 10 è l'unica versione di Windows che supporta SMB 3.1.

SMB 3.1 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione dell'offload delle copie ODX**

L'offload delle copie ODX viene utilizzato automaticamente dai client Windows che lo supportano. Questa opzione è attivata per impostazione predefinita.

- **Abilitazione o disabilitazione del meccanismo di copia diretta per l'offload delle copie ODX**

Il meccanismo di copia diretta aumenta le prestazioni dell'operazione di offload delle copie quando i client Windows tentano di aprire il file di origine di una copia in una modalità che impedisce la modifica del file mentre la copia è in corso. Per impostazione predefinita, il meccanismo di copia diretta è attivato.

- **Abilitazione o disabilitazione dei riferimenti automatici ai nodi**

Con i riferimenti automatici ai nodi, il server SMB fa automaticamente riferimento ai client a una LIF di dati locale al nodo che ospita i dati a cui si accede attraverso la condivisione richiesta.

- **Attivazione o disattivazione delle policy di esportazione per SMB**

Questa opzione è disattivata per impostazione predefinita.

- **Abilitazione o disabilitazione dell'utilizzo dei punti di giunzione come punti di analisi**

Se questa opzione è attivata, il server SMB espone i punti di giunzione ai client SMB come punti di analisi. Questa opzione è valida solo per connessioni SMB 2.x o SMB 3.0. Questa opzione è attivata per impostazione predefinita.

Questa opzione è supportata solo sulle SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Configurazione del numero massimo di operazioni simultanee per connessione TCP**

Il valore predefinito è 255.

- **Abilitazione o disabilitazione della funzionalità locale di utenti e gruppi Windows**

Questa opzione è attivata per impostazione predefinita.

- **Attivazione o disattivazione dell'autenticazione degli utenti Windows locali**

Questa opzione è attivata per impostazione predefinita.

- **Attivazione o disattivazione della funzionalità di copia shadow VSS**

ONTAP utilizza la funzionalità di copia shadow per eseguire backup remoti dei dati memorizzati utilizzando la soluzione Hyper-V su SMB.

Questa opzione è supportata solo sulle SVM e solo per le configurazioni Hyper-V su SMB. L'opzione è attivata per impostazione predefinita sulle SVM

- **Configurazione della profondità della directory della copia shadow**

La configurazione di questa opzione consente di definire la profondità massima delle directory in cui creare copie shadow quando si utilizza la funzionalità di copia shadow.

Questa opzione è supportata solo sulle SVM e solo per le configurazioni Hyper-V su SMB. L'opzione è attivata per impostazione predefinita sulle SVM

- **Attivazione o disattivazione delle funzionalità di ricerca multidominio per la mappatura dei nomi**

Se questa opzione è attivata, quando un utente UNIX viene mappato a un utente di dominio Windows utilizzando un carattere jolly (*) nella parte di dominio del nome utente Windows (ad esempio, * joe), ONTAP ricerca l'utente specificato in tutti i domini con trust bidirezionali nel dominio principale. Il dominio principale è il dominio che contiene l'account del computer del server SMB.

In alternativa alla ricerca di tutti i domini trusted bidirezionalmente, è possibile configurare un elenco di domini trusted preferiti. Se questa opzione è attivata e viene configurato un elenco preferito, l'elenco preferito viene utilizzato per eseguire ricerche di mappatura dei nomi di più domini.

L'impostazione predefinita prevede l'attivazione delle ricerche di associazione dei nomi a più domini.

- **Configurazione della dimensione del settore del file system**

La configurazione di questa opzione consente di configurare la dimensione del settore del file system in byte che ONTAP invia ai client SMB. Sono disponibili due valori validi per questa opzione: 4096 e 512. Il valore predefinito è 4096. Potrebbe essere necessario impostare questo valore su 512 Se l'applicazione Windows supporta solo una dimensione di settore di 512 byte.

- **Attivazione o disattivazione del controllo dinamico degli accessi**

L'attivazione di questa opzione consente di proteggere gli oggetti sul server SMB utilizzando il controllo dinamico dell'accesso (DAC), incluso l'utilizzo del controllo per organizzare i criteri di accesso centrali e l'utilizzo degli oggetti Criteri di gruppo per implementare i criteri di accesso centrali. L'opzione è disattivata per impostazione predefinita.

Questa opzione è supportata solo sulle SVM.

- **Impostazione delle restrizioni di accesso per le sessioni non autenticate (limitazione anonima)**

L'impostazione di questa opzione determina le restrizioni di accesso per le sessioni non autenticate. Le restrizioni vengono applicate agli utenti anonimi. Per impostazione predefinita, non esistono restrizioni di accesso per gli utenti anonimi.

- **Abilitazione o disabilitazione della presentazione di ACL NTFS su volumi con sicurezza efficace UNIX (volumi di sicurezza UNIX o volumi di sicurezza misti con sicurezza effettiva UNIX)**

L'attivazione o la disattivazione di questa opzione determina il modo in cui la sicurezza dei file su file e cartelle con protezione UNIX viene presentata ai client SMB. Se abilitato, ONTAP presenta file e cartelle in volumi con protezione UNIX ai client SMB come dotati di protezione dei file NTFS con ACL NTFS. Se disattivato, ONTAP presenta i volumi con sicurezza UNIX come volumi FAT, senza alcuna protezione dei file. Per impostazione predefinita, i volumi presentano la protezione dei file NTFS con ACL NTFS.

- **Abilitazione o disabilitazione della funzionalità SMB finta aperta**

L'abilitazione di questa funzionalità migliora le performance di SMB 2.x e SMB 3.0 ottimizzando il modo in cui ONTAP effettua richieste aperte e ravvicinato quando si esegue una query per ottenere informazioni sugli attributi su file e directory. Per impostazione predefinita, la funzionalità SMB fake open è attivata. Questa opzione è utile solo per le connessioni effettuate con SMB 2.x o versioni successive.

- **Abilitazione o disabilitazione delle estensioni UNIX**

L'attivazione di questa opzione attiva le estensioni UNIX su un server SMB. Le estensioni UNIX consentono di visualizzare la sicurezza in stile POSIX/UNIX tramite il protocollo SMB. Per impostazione predefinita, questa opzione è disattivata.

Se si dispone di client SMB basati su UNIX, come i client Mac OSX, è necessario attivare le estensioni UNIX. L'abilitazione delle estensioni UNIX consente al server SMB di trasmettere le informazioni di sicurezza POSIX/UNIX tramite SMB al client basato su UNIX, che quindi traduce le informazioni di sicurezza in sicurezza POSIX/UNIX.

- **Abilitazione o disabilitazione del supporto per le ricerche di nomi brevi**

L'attivazione di questa opzione consente al server SMB di eseguire ricerche sui nomi brevi. Una query di ricerca con questa opzione attivata tenta di associare 8.3 nomi di file con nomi di file lunghi. Il valore

predefinito per questo parametro è `false`.

- **Abilitazione o disabilitazione del supporto per la pubblicità automatica delle funzionalità DFS**

L'attivazione o la disattivazione di questa opzione determina se i server SMB pubblicizzano automaticamente le funzionalità DFS ai client SMB 2.x e SMB 3.0 che si connettono alle condivisioni. ONTAP utilizza i riferimenti DFS nell'implementazione di collegamenti simbolici per l'accesso SMB. Se attivato, il server SMB comunica sempre le funzionalità DFS indipendentemente dall'attivazione dell'accesso tramite collegamento simbolico. Se disattivato, il server SMB comunica le funzionalità DFS solo quando i client si connettono alle condivisioni in cui è attivato l'accesso al collegamento simbolico.

- **Configurazione del numero massimo di crediti SMB**

A partire da ONTAP 9.4, configurazione di `-max-credits`. L'opzione consente di limitare il numero di crediti da concedere su una connessione SMB quando client e server eseguono SMB versione 2 o successiva. Il valore predefinito è 128.

- **Abilitazione o disabilitazione del supporto per SMB multicanale**

Attivazione di `-is-multichannel-enabled`. L'opzione di ONTAP 9.4 e versioni successive consente al server SMB di stabilire più connessioni per una singola sessione SMB quando vengono implementate le NIC appropriate sul cluster e sui relativi client. In questo modo si migliora il throughput e la tolleranza agli errori. Il valore predefinito per questo parametro è `false`.

Quando SMB Multichannel è attivato, è anche possibile specificare i seguenti parametri:

- Numero massimo di connessioni consentite per sessione multicanale. Il valore predefinito per questo parametro è 32.
- Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. Il valore predefinito per questo parametro è 256.

Configurare le opzioni del server SMB in ONTAP

È possibile configurare le opzioni del server SMB in qualsiasi momento dopo aver creato un server SMB su una macchina virtuale di storage (SVM).

Fase

1. Eseguire l'azione desiderata:

Se si desidera configurare le opzioni del server SMB...	Immettere il comando...
A livello di privilegi di amministratore	<code>vserver cifs options modify -vserver <i>vserver_name</i> <i>options</i></code>
A livello di privilegi avanzati	<ol style="list-style-type: none"><code>set -privilege advanced</code><code>vserver cifs options modify -vserver <i>vserver_name</i> <i>options</i></code><code>set -privilege admin</code>

Per ulteriori informazioni sulle opzioni del server SMB e sulla `vserver cifs options modify` ["Riferimento al comando ONTAP"](#) loro configurazione, vedere .

Configurare l'autorizzazione del gruppo UNIX per gli utenti SMB di ONTAP

È possibile configurare questa opzione in modo da concedere ai gruppi le autorizzazioni di accesso ai file o alle directory anche se l'utente SMB in entrata non è il proprietario del file.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): set -privilege advanced
2. Configurare l'autorizzazione Grant UNIX group come appropriato:

Se lo si desidera	Immettere il comando
Abilitare l'accesso ai file o alle directory per ottenere le autorizzazioni di gruppo anche se l'utente non è il proprietario del file	vserver cifs options modify -grant-unix-group-perms-to-others true
Disattivare l'accesso ai file o alle directory per ottenere le autorizzazioni di gruppo anche se l'utente non è il proprietario del file	vserver cifs options modify -grant-unix-group-perms-to-others false

3. Verificare che l'opzione sia impostata sul valore desiderato: vserver cifs options show -fields grant-unix-group-perms-to-others
4. Tornare al livello di privilegio admin: set -privilege admin

Configurare le restrizioni di accesso SMB a ONTAP per utenti anonimi

Per impostazione predefinita, un utente anonimo e non autenticato (noto anche come *null user*) può accedere a determinate informazioni sulla rete. È possibile utilizzare un'opzione del server SMB per configurare le restrizioni di accesso per l'utente anonimo.

A proposito di questa attività

Il `-restrict-anonymous` L'opzione del server SMB corrisponde a. `RestrictAnonymous` Voce di registro in Windows.

Gli utenti anonimi possono elencare o enumerare determinati tipi di informazioni di sistema dagli host Windows sulla rete, inclusi i nomi e i dettagli degli utenti, i criteri degli account e i nomi di condivisione. È possibile controllare l'accesso per l'utente anonimo specificando una delle tre impostazioni di restrizione dell'accesso:

Valore	Descrizione
no-restriction (impostazione predefinita)	Non specifica restrizioni di accesso per utenti anonimi.
no-enumeration	Specifica che solo l'enumerazione è limitata per gli utenti anonimi.
no-access	Specifica che l'accesso è limitato agli utenti anonimi.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): set -privilege advanced
2. Configurare l'impostazione limita anonimo: vserver cifs options modify -vserver *vserver_name* -restrict-anonymous {no-restriction|no-enumeration|no-access}
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 correlate

[Opzioni server disponibili](#)

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 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.