



Proteggere l'accesso ai file utilizzando i permessi

ONTAP 9

NetApp
April 24, 2024

Sommario

- Proteggere l'accesso ai file utilizzando i permessi 1
 - Configurare le autorizzazioni avanzate per i file NTFS utilizzando la scheda protezione di Windows 1
 - Configurare le autorizzazioni per i file NTFS utilizzando l'interfaccia utente di ONTAP. 4
 - In che modo le autorizzazioni dei file UNIX forniscono il controllo degli accessi quando si accede ai file tramite SMB 4

Proteggere l'accesso ai file utilizzando i permessi

Configurare le autorizzazioni avanzate per i file NTFS utilizzando la scheda protezione di Windows

È possibile configurare le autorizzazioni standard per i file NTFS su file e cartelle utilizzando la scheda **Windows Security** nella finestra Proprietà di Windows.

Prima di iniziare

L'amministratore che esegue questa attività deve disporre di autorizzazioni NTFS sufficienti per modificare le autorizzazioni sugli oggetti selezionati.

A proposito di questa attività

La configurazione delle autorizzazioni dei file NTFS viene eseguita su un host Windows aggiungendo voci agli elenchi di controllo degli accessi discrezionali (DACL) NTFS associati a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS. Queste attività vengono gestite automaticamente dalla GUI di Windows.

Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la finestra di dialogo **Map Network Drive** (Connetti unità di rete):
 - a. Selezionare una lettera **Drive**.
 - b. Nella casella **Folder**, digitare il nome del server CIFS contenente la condivisione contenente i dati a cui si desidera applicare le autorizzazioni e il nome della condivisione.

Se il nome del server CIFS è "CIFS_SERVER" e la condivisione è denominata "share1", digitare \\CIFS_SERVER\share1.



È possibile specificare l'indirizzo IP dell'interfaccia dati per il server CIFS invece del nome del server CIFS.

- c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui si desidera impostare le autorizzazioni per il file NTFS.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory, quindi selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.

La scheda **Security** visualizza l'elenco di utenti e gruppi per i quali è impostata l'autorizzazione NTFS. La casella **Permissions for** (autorizzazioni per) visualizza un elenco delle autorizzazioni Allow e Nega in vigore per ogni utente o gruppo selezionato.

6. Fare clic su **Avanzate**.

La finestra Proprietà di Windows visualizza informazioni sulle autorizzazioni file esistenti assegnate a utenti

e gruppi.

7. Fare clic su **Modifica permessi**.

Viene visualizzata la finestra Permissions (autorizzazioni).

8. Eseguire le azioni desiderate:

Se si desidera...	Effettuare le seguenti operazioni...
Impostare autorizzazioni NTFS avanzate per un nuovo utente o gruppo	<ul style="list-style-type: none">a. Fare clic su Aggiungi.b. Nella casella inserire il nome dell'oggetto da selezionare, digitare il nome dell'utente o del gruppo che si desidera aggiungere.c. Fare clic su OK.
Modificare le autorizzazioni NTFS avanzate da un utente o da un gruppo	<ul style="list-style-type: none">a. Nella casella Permissions entries:, selezionare l'utente o il gruppo di cui si desidera modificare le autorizzazioni avanzate.b. Fare clic su Edit (Modifica).
Rimuovere le autorizzazioni NTFS avanzate per un utente o un gruppo	<ul style="list-style-type: none">a. Nella casella Permissions entries:, selezionare l'utente o il gruppo che si desidera rimuovere.b. Fare clic su Rimuovi.c. Passare alla fase 13.

Se si aggiungono autorizzazioni NTFS avanzate a un nuovo utente o gruppo o si modificano le autorizzazioni avanzate NTFS per un utente o un gruppo esistente, viene visualizzata la finestra immissione autorizzazioni per <Object>.

9. Nella casella **Apply to** (Applica a), selezionare la modalità di applicazione della voce di autorizzazione del file NTFS.

Se si impostano le autorizzazioni per un file NTFS su un singolo file, la casella **Apply to** (Applica a) non è attiva. L'impostazione predefinita di **Apply to** (Applica a) è **solo questo oggetto**.

10. Nella casella **Permissions** (autorizzazioni), selezionare le caselle **Allow** (Consenti) o **Nega** per le autorizzazioni avanzate che si desidera impostare su questo oggetto.

- Per consentire l'accesso specificato, selezionare la casella **allow**.
- Per non consentire l'accesso specificato, selezionare la casella **Nega**. È possibile impostare le autorizzazioni per i seguenti diritti avanzati:

- **Controllo completo**

Se si sceglie questo diritto avanzato, tutti gli altri diritti avanzati vengono scelti automaticamente (diritti Allow o Nega).

- **Cartella Traverse / file di esecuzione**
- **Elenca cartella / leggi dati**

- **Attributi di lettura**
- **Leggi attributi estesi**
- **Creare file / scrivere dati**
- **Crea cartelle/Aggiungi dati**
- **Attributi di scrittura**
- **Scrivi attributi estesi**
- **Elimina sottocartelle e file**
- **Elimina**
- **Permessi di lettura**
- **Modifica delle autorizzazioni**
- **Assumere la proprietà**



Se una delle caselle di autorizzazione avanzate non è selezionabile, le autorizzazioni vengono ereditate dall'oggetto padre.

11. Se si desidera che le sottocartelle e i file di questo oggetto ereditino queste autorizzazioni, selezionare la casella **Applica queste autorizzazioni solo agli oggetti e/o ai contenitori all'interno di questo contenitore**.
12. Fare clic su **OK**.
13. Dopo aver aggiunto, rimosso o modificato le autorizzazioni NTFS, specificare l'impostazione di ereditarietà per questo oggetto:

- Selezionare la casella **include inheritable permissions from this object's parent**.

Questa è l'impostazione predefinita.

- Selezionare la casella **Sostituisci tutte le autorizzazioni dell'oggetto figlio con le autorizzazioni ereditabili da questo oggetto**.

Questa impostazione non è presente nella casella permessi se si impostano i permessi del file NTFS su un singolo file.



Fare attenzione quando si seleziona questa impostazione. Questa impostazione rimuove tutte le autorizzazioni esistenti su tutti gli oggetti figlio e le sostituisce con le impostazioni di autorizzazione dell'oggetto. È possibile rimuovere inavvertitamente le autorizzazioni che non si desidera rimuovere. È particolarmente importante quando si impostano le autorizzazioni in un volume misto di sicurezza o in un qtree. Se gli oggetti figlio dispongono di uno stile di protezione UNIX effettivo, la propagazione delle autorizzazioni NTFS a tali oggetti figlio comporta la modifica di tali oggetti da stile di protezione UNIX a stile di protezione NTFS da parte di ONTAP e la sostituzione di tutte le autorizzazioni UNIX per tali oggetti figlio con autorizzazioni NTFS.

- Selezionare entrambe le caselle.
- Selezionare nessuna delle due caselle.

14. Fare clic su **OK** per chiudere la casella **Permissions**.
15. Fare clic su **OK** per chiudere la casella **Impostazioni di protezione avanzate per <Object>**.

Per ulteriori informazioni su come impostare le autorizzazioni NTFS avanzate, consultare la documentazione di Windows.

Informazioni correlate

[Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI](#)

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security](#)

[Visualizzazione di informazioni sulla sicurezza dei file su volumi misti di tipo sicurezza](#)

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi UNIX di tipo Security](#)

Configurare le autorizzazioni per i file NTFS utilizzando l'interfaccia utente di ONTAP

È possibile configurare le autorizzazioni dei file NTFS su file e directory utilizzando l'interfaccia utente di ONTAP. Ciò consente di configurare le autorizzazioni per i file NTFS senza la necessità di connettersi ai dati utilizzando una condivisione SMB su un client Windows.

È possibile configurare le autorizzazioni dei file NTFS aggiungendo voci agli elenchi di controllo degli accessi discrezionali (DACL) NTFS associati a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS.

È possibile configurare le autorizzazioni dei file NTFS solo dalla riga di comando. Non è possibile configurare gli ACL NFSv4 utilizzando l'interfaccia CLI.

Fasi

1. Creare un descrittore di protezione NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. Aggiungere DACL al descrittore di protezione NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. Creare una policy di sicurezza per file/directory.

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

In che modo le autorizzazioni dei file UNIX forniscono il controllo degli accessi quando si accede ai file tramite SMB

Un volume FlexVol può avere uno dei tre tipi di protezione: NTFS, UNIX o misto. È

possibile accedere ai dati tramite SMB indipendentemente dallo stile di sicurezza; tuttavia, sono necessarie autorizzazioni appropriate per i file UNIX per accedere ai dati con una protezione efficace UNIX.

Quando si accede ai dati tramite SMB, vengono utilizzati diversi controlli di accesso per determinare se un utente è autorizzato a eseguire un'azione richiesta:

- Permessi di esportazione

La configurazione delle autorizzazioni di esportazione per l'accesso SMB è facoltativa.

- Autorizzazioni di condivisione
- Permessi del file

I seguenti tipi di permessi di file potrebbero essere applicati ai dati sui quali l'utente desidera eseguire un'azione:

- NTFS
- ACL NFSv4 UNIX
- Bit di modalità UNIX

Per i dati con ACL NFSv4 o bit di modalità UNIX impostati, vengono utilizzate autorizzazioni di stile UNIX per determinare i diritti di accesso ai dati. L'amministratore di SVM deve impostare l'autorizzazione file appropriata per garantire che gli utenti dispongano dei diritti per eseguire l'azione desiderata.



I dati in un volume misto di sicurezza potrebbero avere uno stile di sicurezza efficace NTFS o UNIX. Se i dati hanno uno stile di sicurezza UNIX effettivo, le autorizzazioni NFSv4 o i bit di modalità UNIX vengono utilizzati per determinare i diritti di accesso ai dati.

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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.