



Configurare l'accesso del client SMB allo storage condiviso

ONTAP 9

NetApp
April 24, 2024

Sommario

- Configurare l'accesso del client SMB allo storage condiviso 1
 - Configurare l'accesso del client SMB allo storage condiviso 1
 - Creare un volume o un contenitore di storage qtree 1
 - Requisiti e considerazioni per la creazione di una condivisione SMB 4
 - Creare una condivisione SMB 5
 - Verificare l'accesso al client SMB 6
 - Creare elenchi di controllo degli accessi di condivisione SMB 6
 - Configurare le autorizzazioni per i file NTFS in una condivisione 8
 - Verificare l'accesso dell'utente 10

Configurare l'accesso del client SMB allo storage condiviso

Configurare l'accesso del client SMB allo storage condiviso

Per fornire l'accesso del client SMB allo storage condiviso su una SVM, è necessario creare un volume o un qtree per fornire un container di storage, quindi creare o modificare una condivisione per tale container. È quindi possibile configurare le autorizzazioni di condivisione e file e verificare l'accesso dai sistemi client.

Prima di iniziare

- SMB deve essere completamente configurato sulla SVM.
- Tutti gli aggiornamenti della configurazione dei name service devono essere completati.
- Eventuali aggiunte o modifiche a un dominio Active Directory o alla configurazione del gruppo di lavoro devono essere completate.

Creare un volume o un contenitore di storage qtree

Creare un volume

È possibile creare un volume e specificarne il punto di giunzione e altre proprietà utilizzando `volume create` comando.

A proposito di questa attività

Un volume deve includere un *percorso di giunzione* per rendere i dati disponibili ai client. È possibile specificare il percorso di giunzione quando si crea un nuovo volume. Se si crea un volume senza specificare un percorso di giunzione, è necessario *montare* il volume nello spazio dei nomi SVM utilizzando `volume mount` comando.

Prima di iniziare

- SMB deve essere configurato e funzionante.
- Lo stile di sicurezza SVM deve essere NTFS.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).

Fasi

1. Creare il volume con un punto di giunzione: `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path`

Le scelte per `-junction-path` sono i seguenti:

- Direttamente sotto root, ad esempio /new_vol

È possibile creare un nuovo volume e specificarne il montaggio direttamente nel volume root SVM.

- In una directory esistente, ad esempio /existing_dir/new_vol

È possibile creare un nuovo volume e specificarne il montaggio in un volume esistente (in una gerarchia esistente), espresso come directory.

Se si desidera creare un volume in una nuova directory (in una nuova gerarchia sotto un nuovo volume), ad esempio, /new_dir/new_vol, Quindi, è necessario creare prima un nuovo volume padre che sia congiunto al volume root SVM. Creare quindi il nuovo volume figlio nel percorso di giunzione del nuovo volume padre (nuova directory).

2. Verificare che il volume sia stato creato con il punto di giunzione desiderato: `volume show -vserver svm_name -volume volume_name -junction`

Esempi

Il seguente comando crea un nuovo volume denominato users1 su SVM vs1.example.com e sull'aggregato aggr1. Il nuovo volume è disponibile all'indirizzo /users. Il volume ha una dimensione di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

Il seguente comando crea un nuovo volume denominato "home4" su SVM "vs1.example.com" e l'aggregato "aggr1". La directory /eng/ Esiste già nello spazio dei nomi per vs1 SVM e il nuovo volume è disponibile all'indirizzo /eng/home, che diventa la home directory di /eng/ namespace. Il volume è di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

Creare un qtree

È possibile creare un qtree per contenere i dati e specificarne le proprietà utilizzando volume qtree create comando.

Prima di iniziare

- La SVM e il volume che conterrà il nuovo qtree devono già esistere.
- Lo stile di sicurezza SVM deve essere NTFS e SMB deve essere configurato e in esecuzione.

Fasi

1. Creare il qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

È possibile specificare il volume e il qtree come argomenti separati o specificare l'argomento del percorso qtree nel formato `/vol/volume_name/_qtree_name`.

2. Verificare che il qtree sia stato creato con il percorso di giunzione desiderato: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Esempio

Nell'esempio seguente viene creato un qtree chiamato qt01 situato su SVM vs1.example.com che ha un percorso di giunzione `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```

Vserver Name: vs1.example.com
Volume Name: data1
Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
Security Style: ntfs
Oplock Mode: enable
Unix Permissions: ---rwxr-xr-x
Qtree Id: 2
Qtree Status: normal
Export Policy: default
Is Export Policy Inherited: true
```

Requisiti e considerazioni per la creazione di una condivisione SMB

Prima di creare una condivisione SMB, è necessario comprendere i requisiti per i percorsi di condivisione e le proprietà di condivisione, in particolare per le home directory.

La creazione di una condivisione SMB richiede la specifica di una struttura di percorso di directory (utilizzando l' `-path` in `vserver cifs share create` a cui accederanno i client. Il percorso della directory corrisponde al percorso di giunzione di un volume o `qtree` creato nello spazio dei nomi SVM. Il percorso di directory e il percorso di giunzione corrispondente devono esistere prima di creare la condivisione.

I percorsi di condivisione hanno i seguenti requisiti:

- Il nome di un percorso di directory può contenere fino a 255 caratteri.
- Se nel nome del percorso è presente uno spazio, l'intera stringa deve essere inserita tra virgolette (ad esempio, `"/new volume/mount here"`).
- Se il percorso UNC (`\\servername\sharename\filepath`) Della condivisione contiene più di 256 caratteri (escludendo l'iniziale `""` nel percorso UNC), quindi la scheda **Security** nella casella Proprietà di Windows non è disponibile.

Si tratta di un problema del client Windows piuttosto che di un problema ONTAP. Per evitare questo problema, non creare condivisioni con percorsi UNC con più di 256 caratteri.

È possibile modificare le impostazioni predefinite della proprietà di condivisione:

- Le proprietà iniziali predefinite per tutte le condivisioni sono `oplocks`, `browsable`, `changenotify`, e `show-previous-versions`.
- È facoltativo specificare le proprietà di condivisione quando si crea una condivisione.

Tuttavia, se si specificano le proprietà di condivisione quando si crea la condivisione, le impostazioni predefinite non vengono utilizzate. Se si utilizza `-share-properties` parametro quando si crea una condivisione, è necessario specificare tutte le proprietà della condivisione che si desidera applicare alla condivisione utilizzando un elenco delimitato da virgole.

- Per designare una condivisione della home directory, utilizzare `homedirectory` proprietà.

Questa funzione consente di configurare una condivisione mappata a diverse directory in base all'utente che si connette ad essa e a una serie di variabili. Invece di dover creare condivisioni separate per ciascun utente, è possibile configurare una singola condivisione con alcuni parametri della home directory per definire la relazione di un utente tra un punto di ingresso (la condivisione) e la propria home directory (una directory sulla SVM).



Non è possibile aggiungere o rimuovere questa proprietà dopo aver creato la condivisione.

Le condivisioni home directory hanno i seguenti requisiti:

- Prima di creare le home directory SMB, è necessario aggiungere almeno un percorso di ricerca della home directory utilizzando `vserver cifs home-directory search-path add` comando.
- Condivisioni home directory specificate dal valore di `homedirectory` su `-share-properties` il parametro deve includere `%w` (Nome utente Windows) variabile dinamica nel nome della condivisione.

Il nome della condivisione può contenere anche %d (nome di dominio) variabile dinamica (ad esempio, %d/%w) o una parte statica nel nome della condivisione (ad esempio, home1_%w).

- Se la condivisione viene utilizzata da amministratori o utenti per connettersi alle home directory di altri utenti (utilizzando le opzioni di `vserver cifs home-directory modify` comando), il modello di nome di condivisione dinamica deve essere preceduto da una tilde (~).

"[Gestione delle PMI](#)" e `vserver cifs share` le pagine man contengono informazioni aggiuntive.

Creare una condivisione SMB

È necessario creare una condivisione SMB prima di poter condividere i dati da un server SMB con client SMB. Quando si crea una condivisione, è possibile impostare le proprietà della condivisione, ad esempio designarla come home directory. È inoltre possibile personalizzare la condivisione configurando le impostazioni opzionali.

Prima di iniziare

Il percorso della directory per il volume o qtree deve esistere nello spazio dei nomi SVM prima di creare la condivisione.

A proposito di questa attività

Quando si crea una condivisione, l'ACL di condivisione predefinito (autorizzazioni di condivisione predefinite) è Everyone / Full Control. Dopo aver testato l'accesso alla condivisione, rimuovere l'ACL della condivisione predefinita e sostituirlo con un'alternativa più sicura.

Fasi

1. Se necessario, creare la struttura del percorso di directory per la condivisione.

Il `vserver cifs share create` il comando verifica il percorso specificato in `-path` durante la creazione della condivisione. Se il percorso specificato non esiste, il comando non riesce.

2. Creare una condivisione SMB associata alla SVM specificata: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verificare che la condivisione sia stata creata: `vserver cifs share show -share-name share_name`

Esempi

Il seguente comando crea una condivisione SMB denominata "SHARE1" su SVM `vs1.example.com`. Il percorso della directory è `/users` e viene creato con le proprietà predefinite.

```
cluster1::> vsriver cifs share create -vsriver vs1.example.com -share-name  
SHARE1 -path /users
```

```
cluster1::> vsriver cifs share show -share-name SHARE1
```

Vsriver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full
Control			browsable		
			changenotify		
			show-previous-versions		

Verificare l'accesso al client SMB

Verificare di aver configurato SMB correttamente accedendo e scrivendo i dati nella condivisione. Verificare l'accesso utilizzando il nome del server SMB e gli alias NetBIOS.

Fasi

1. Accedere a un client Windows.
2. Verificare l'accesso utilizzando il nome del server SMB:
 - a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato: `\\SMB_Server_Name\Share_Name`

Se la mappatura non riesce, è possibile che la mappatura DNS non sia ancora propagata in tutta la rete. È necessario verificare l'accesso utilizzando il nome del server SMB in un secondo momento.

Se il server SMB è denominato `vs1.example.com` e la condivisione è denominata `SHARE1`, immettere quanto segue: `\\vs0.example.com\SHARE1`
 - b. Sul disco appena creato, creare un file di prova, quindi eliminare il file.

L'accesso in scrittura alla condivisione è stato verificato utilizzando il nome del server SMB.
3. Ripetere il passaggio 2 per tutti gli alias NetBIOS.

Creare elenchi di controllo degli accessi di condivisione SMB

La configurazione delle autorizzazioni di condivisione mediante la creazione di elenchi di controllo degli accessi (ACL) per le condivisioni SMB consente di controllare il livello di accesso a una condivisione per utenti e gruppi.

Prima di iniziare

È necessario decidere quali utenti o gruppi avranno accesso alla condivisione.

A proposito di questa attività

È possibile configurare gli ACL a livello di condivisione utilizzando nomi di utenti o gruppi Windows locali o di dominio.

Prima di creare un nuovo ACL, è necessario eliminare l'ACL di condivisione predefinito `Everyone / Full Control`, che comporta un rischio per la sicurezza.

In modalità workgroup, il nome di dominio locale è il nome del server SMB.

Fasi

- 1. Eliminare l'ACL di condivisione predefinito:
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
- 2. Configurare il nuovo ACL:

Se si desidera configurare gli ACL utilizzando un...	Immettere il comando...
Utente Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</code>
Gruppo di Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</code>

- 3. Verificare che l'ACL applicato alla condivisione sia corretto utilizzando `vserver cifs share access-control show` comando.

Esempio

Il seguente comando fornisce Change Autorizzazioni al gruppo Windows "Sales Team" per la condivisione "sales" su "`vs1.example.com`SVM`":

```
cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsserver cifs share access-control show
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

I seguenti comandi impartire Change Autorizzazione al gruppo Windows locale denominato "Tiger Team" e Full_Control Autorizzazione all'utente Windows locale denominato "Sue Chang" per la condivisione "datavol5" su "vs1" SVM:

```
cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsserver cifs share access-control show -vsserver vs1
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

Configurare le autorizzazioni per i file NTFS in una condivisione

Per consentire l'accesso ai file agli utenti o ai gruppi che hanno accesso a una condivisione, è necessario configurare le autorizzazioni dei file NTFS su file e directory in tale condivisione da un client 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

"[Gestione delle PMI](#)" La documentazione di Windows contiene informazioni su come impostare le autorizzazioni NTFS standard e avanzate.

Fasi

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

Se il nome del server SMB è SMB_SERVER01 e la condivisione è denominata "SHARE1", immettere \\SMB_SERVER01\SHARE1.



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

- 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.

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

La scheda Security (sicurezza) visualizza l'elenco di utenti e gruppi per i quali è impostata l'autorizzazione NTFS. La casella Permissions for <Object> (autorizzazioni per utenti) visualizza un elenco di permessi e permessi di negazione in vigore per l'utente o il gruppo selezionato.

7. Fare clic su **Edit** (Modifica).

Viene visualizzata la finestra Permissions for <Object> (autorizzazioni per l'accesso)

8. Eseguire le azioni desiderate:

Se si desidera	Effettuare le seguenti operazioni...
Impostare le autorizzazioni NTFS standard per un nuovo utente o gruppo	<p>a. Fare clic su Aggiungi.</p> <p>Viene visualizzata la finestra Seleziona utente, computer, account di servizio o gruppi.</p> <p>b. Nella casella inserire i nomi degli oggetti da selezionare, digitare il nome dell'utente o del gruppo a cui si desidera aggiungere l'autorizzazione NTFS.</p> <p>c. Fare clic su OK.</p>
Modificare o rimuovere le autorizzazioni NTFS standard da un utente o gruppo	Nella casella nomi gruppo o utente , selezionare l'utente o il gruppo che si desidera modificare o rimuovere.

9. Eseguire le azioni desiderate:

Se si desidera...	Effettuare le seguenti operazioni
Impostare le autorizzazioni NTFS standard per un utente o un gruppo nuovo o esistente	Nella casella Permissions for <Object> (autorizzazioni per l'accesso), selezionare le caselle Allow (Consenti) o Nega per il tipo di accesso che si desidera consentire o meno per l'utente o il gruppo selezionato.
Rimuovere un utente o un gruppo	Fare clic su Rimuovi .



Se alcune o tutte le caselle di autorizzazione standard non sono selezionabili, le autorizzazioni vengono ereditate dall'oggetto padre. La casella **permessi speciali** non è selezionabile. Se selezionata, significa che uno o più diritti avanzati granulari sono stati impostati per l'utente o il gruppo selezionato.

10. Una volta aggiunte, rimosse o modificate le autorizzazioni NTFS per l'oggetto, fare clic su **OK**.

Verificare l'accesso dell'utente

È necessario verificare che gli utenti configurati possano accedere alla condivisione SMB e ai file in essa contenuti.

Fasi

1. Su un client Windows, accedere come uno degli utenti che ora ha accesso alla condivisione.
2. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
3. Completare la casella **Map Network Drive** (Connetti unità di rete):
 - a. Selezionare una lettera **Drive**.
 - b. Nella casella **Folder** (cartella), digitare il nome della condivisione che verrà fornito agli utenti.

Se il nome del server SMB è SMB_SERVER01 e la condivisione è denominata "SHARE1", immettere \\SMB_SERVER01\share1.

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.

4. Creare un file di test, verificare che esista, scriverne del testo e rimuovere il file di test.

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.