

Consentire agli utenti di recuperare i propri file in autonomia con le Shadow Copies of Shared Folders.

Da PierGiorgio Malusardi (MCSE – MCSA – MCT) - IT Pro Evangelist Microsoft Italia

Uno dei principali motivi di richiesta d'aiuto al supporto IT delle aziende (o al collega più esperto) è la necessità di recuperare file importanti sovrascritti da nuove versioni o cancellati. La situazione classica è quella in cui un utente apre un file contenente, per esempio, un'offerta fatta ad un cliente, la modifica solo in parte per un nuovo cliente e, al momento di salvarla, invece che scegliere la voce di menù Salva con nome, sceglie Salva. A questo punto il danno è fatto: la versione originale è persa! Scatta immediata (in realtà l'immediatezza dipende dalla consapevolezza dell'utente e dai suoi tempi di reazione) la chiamata al supporto con la richiesta di recupero del file, ammesso che lo stesso sia stato salvato in qualche backup.

Questo genera una perdita di tempo, e quindi di produttività, per il diretto interessato e per il personale del supporto. Sarebbe bello se l'utente, con pochi colpi di mouse fosse in grado di recuperare da sé la versione originale del file.

In questa pagina

- ↓ [Introduzione](#)
- ↓ [Configurazione del file server](#)
- ↓ [Configurazione del client](#)
- ↓ [Funzionamento](#)
- ↓ [Conclusioni](#)

Introduzione

Per mitigare i problemi posti dallo scenario descritto ci viene in aiuto la nuova architettura di gestione dei dischi presente in Windows Server 2003 ed in particolare una sua applicazione nota come **Shadow copies of Shared Folders**.

Vediamo, in figura 1, com'è strutturato lo stack di gestione degli storage di Windows Server 2003:

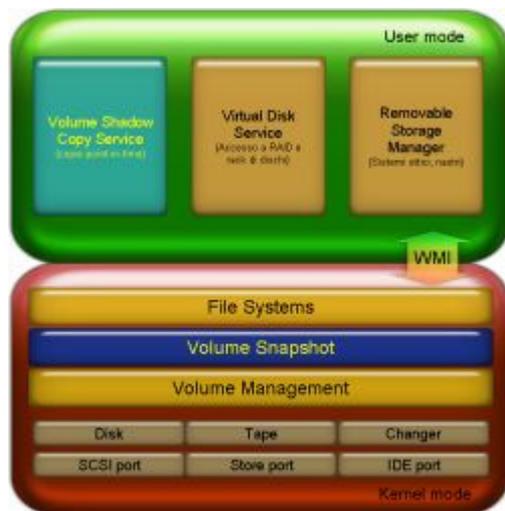


Figura 1.

Le parti della struttura che ci interessano, ai fini del problema che stiamo analizzando, sono il Volume Shadow Copy Service e il Volume Snapshot.

Insieme consentono di effettuare una copia point-in-time dei dati su disco.

È importante notare la posizione del Volume Snapshot: si trova sotto il livello File System e sopra quello di Volume Management. Questa posizione determina la sua "visione dei dati su disco". Il Volume Snapshot non "conosce" il concetto di file, ma "conosce" il concetto di cluster; questo significa che, per il Volume Snapshot, i dati sono una sequenza di cluster senza altra organizzazione che la geometria del disco.

In molte situazioni avere un servizio che non conosce il concetto di "file aperto" è un grosso vantaggio.

Grazie a questa architettura è possibile effettuare degli "snapshot" ossia delle fotografie dello stato del disco (Attenzione non una copia dei dati presenti su disco).

Supponiamo di avere una applicazione che scrive dati su disco e di volere fare una copia di questi dati in un preciso istante e a file aperti.

All'istante desiderato (T1) eseguiamo uno "snapshot" ossia una "fotografia" dei cluster del disco occupati dai dati. Da questo momento in avanti ogni volta che l'applicazione chiede al sistema operativo di modificare un cluster, i vecchi dati contenuti

in questo sono copiati in un'altra porzione del disco detta "area delle differenze" (Diff Area).

La copia dei dati, coerente con T1, sarà costruita leggendo i cluster non modificati dalla loro posizione originaria e i cluster modificati dalla Diff Area. La figura 2 ci può aiutare a comprendere meglio la situazione.

Tempo	Cluster su disco	Diff area
T1	①②③④⑤⑥⑦⑧⑨⑩	
T2	①②③④⑤⑥⑦⑧⑨⑩	④⑤⑥
Copia dei dati coerente con T1		
T2	①②③④⑤⑥⑦⑧⑨⑩	

Questo meccanismo è utilissimo per l'esecuzione di backup di dati residenti in file che non possono essere chiusi e gestiti da applicazioni che non possono essere spente (database, sistemi di posta, ecc...).

Vediamo nel seguito, di questo documento, come questo meccanismo è sfruttato in Windows Server 2003, oltre che per fare backup a file aperti, anche per mantenere diverse versioni dello stesso file e permettere quindi all'utente di recuperare i dati maldestramente persi.

Per una migliore comprensione dei concetti espressi faremo riferimento alla semplice rete esposta in figura 3

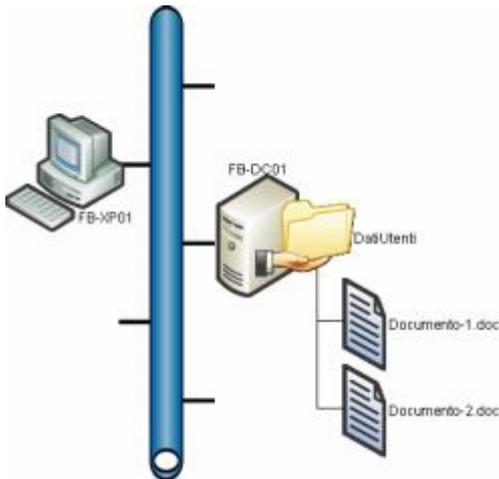


Figura 3.

[Inizio pagina](#)

Configurazione del file server

Per raggiungere il nostro scopo dovremo effettuare delle configurazioni sia sui file server sia sui client della rete.

Il primo passo è creare una struttura di share adatta al salvataggio in rete dei file dei nostri utenti aziendali. Le **Shadow Copies of Shared Folder**, infatti, funzionano solo per i file salvati in share di rete.

A titolo esemplificativo io userò il folder **DatiUtente**, creato sul disco **E:** del mio server e condiviso come **DatiUtente**.

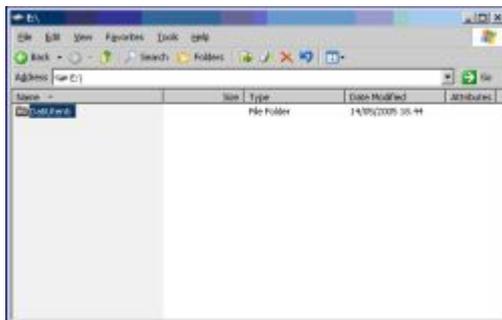


Figura 4.

Il folder contiene due documenti word (Documento-1.doc e Documento-2.doc) nelle loro versioni originali.

A questo punto possiamo abilitare le Shadow Copies. L'abilitazione delle Shadow Copies, come per le Quote disco, può essere fatto solo volume per volume.

Apriamo le proprietà del disco **E:** e, nella finestra di dialogo **Dati (E:) Properties** selezioniamo il tab **Shadow Copies**.

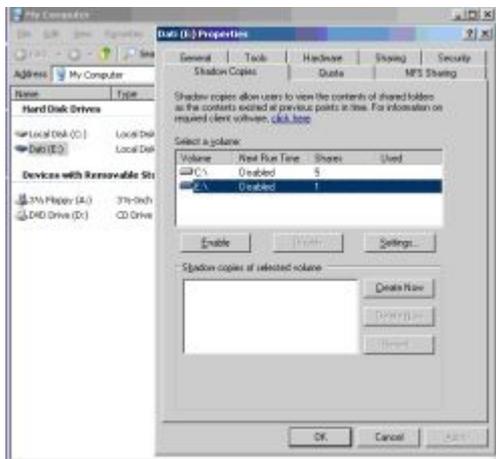


Figura 5.

Analizziamo le opzioni di configurazione disponibili, selezionando il disco E: e cliccando il bottone **Settings** nella dialog box **Data (E:) Properties**.

La prima opzione (figura 6) ci consente di scegliere il disco su cui creare la Diff Area (casella di scelta **Locate on this volume**).

Su server con elevato I/O è buona pratica creare la Diff Area su un disco diverso rispetto a quello dei dati e su cui non si abiliteranno le Shadow Copies (per altre indicazioni vedere il riquadro **Buone pratiche nell'uso delle Shadow Copies of Shared Folder**

Nel mio caso, avendo a disposizione solo il disco di sistema (C:) e il disco dati (E:) creerò la Diff Area quest'ultimo.

La seconda opzione disponibile è la possibilità di impostare lo spazio disco dedicato alla Diff Area (radio button **Maximum size**). Il valore predefinito è il 10% della dimensione del disco dati con un minimo di 300MB. È anche possibile non porre limiti di crescita alle Shadow Copies.

La scelta del disco su cui porre la Diff Area, e la dimensione di questa, deve essere fatta con molta attenzione e dopo un'attenta valutazione. Se, in un secondo tempo, si rendesse necessario modificare queste impostazioni sarà necessario eliminare le Shadow Copies create, perdendo tutte le precedenti versioni dei file.

La scelta della dimensione massima della Diff Area deve essere guidata oltre che dalla dimensione del disco, dal numero di file presenti, dalla loro dimensione e dalla frequenza di modifica degli stessi. Pochi file, modificati frequentemente, determinano una maggiore occupazione di spazio, in Diff Area, di molti file modificati raramente.



Figura 6.

Cliccando il bottone **Schedule**, nella finestra **Settings**, è possibile impostare la frequenza di esecuzione delle Shadow Copies.

Il default è due Shadow Copies al giorno, eseguite alle 7:00 e alle 12:00, tutti i giorni, dal Lunedì al Venerdì.

Anche in questo caso le scelte da effettuare dipendono strettamente dalle modalità di lavoro dei nostri utenti.

Le domande che ci si deve porre nella scelta della frequenza di esecuzione delle Shadow Copies sono:

- La maggior parte dei nostri utenti che orari di lavoro hanno?
- Gli utenti che useranno questo file server sono tutti nello stesso fuso orario?
- Quante ore di lavoro i nostri utenti sono disposti a perdere in caso di perdita di un file?

- Le impostazioni predefinite sono adeguate per i nostri utenti?
- Quanto spesso le Shadow Copies possono essere eseguite senza che si debba aggiungere spazio disco?
- Quanti giorni di storico delle versioni dei file possono essere mantenuti prima di raggiungere il limite di 64 Shadow Copies per volume?



Figura 7.

Cliccando su **New**, nella finestra **E:** (figura 7), si apre la finestra di dialogo che consente di impostare ulteriori eventi di creazione di Shadow Copies.

In alternativa alla creazione di nuovi eventi si può cliccare il bottone **Advanced** e impostare la ripetizione del task selezionato, impostando la frequenza di ripetizione (**Repeat task – Every** in figura 8) e la durata massima di ogni ripetizione (**Duration**).

A questo proposito è bene sottolineare che è consigliato non scendere sotto l'ora di intervallo, tra l'esecuzione di una Shadow Copy e la successiva, per non saturare troppo velocemente la Diff Area (per altre indicazioni vedere il riquadro **Buone pratiche nell'uso delle Shadow Copies of Shared Folder**

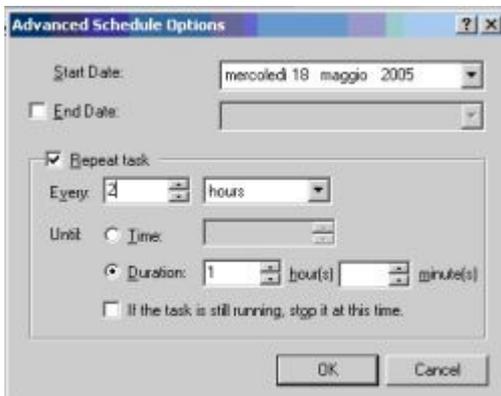


Figura 8.

Abbiamo così terminato la configurazione delle Shadow Copies per il disco E:. Chiudiamo le diverse finestre dei **Settings** premendo il bottone **OK**, presente in ciascuna, e abilitiamo le Shadow Copies per il disco E: cliccando il bottone **Enable** nella finestra di dialogo **Data (E:) Properties** (figura 5).

Appare un messaggio di avviso (figura 9) che ci consiglia, nel caso si stia configurando un server con elevato I/O, di cambiare le impostazioni di default.

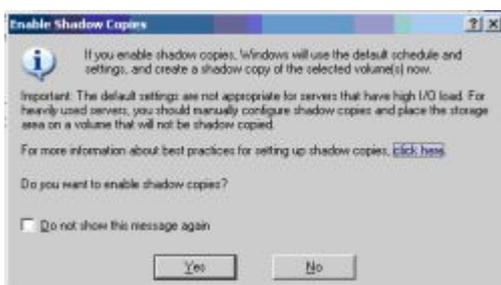


Figura 9.

Nella finestra di avviso clicchiamo su **Yes** per abilitare le Shadows Copies e attendiamo che la prima Shadows Copy venga eseguita.

Il lavoro di configurazione lato server termina qui.

Buone pratiche nell'uso delle Shadow Copies of Shared Folder

In caso di server con elevato I/O è buona pratica selezionare dischi diversi per i dati e per la Diff Area e posizionare quest'ultima su un disco su cui non sono abilitate le Shadow Copies. Altre buone norme sono:

- Non abilitare le Shadow Copies su dischi che usano mount point perché questi ultimi non saranno considerati
- Non abilitare le Shadow Copies su sistemi con dual boot con sistemi pre Windows Server 2003. Questo per evitare che l'avvio del vecchio sistema operativo rovini le Shadow Copies (che sono persistenti e renda impossibile il riavvio con Windows Server 2003)
- Non eseguire Shadow Copies con frequenza inferiore all'ora per evitare di saturare troppo velocemente lo spazio disco dedicato o di provocare una rapida cancellazione di Shadow Copies (c'è un limite di 64 Shadow Copies per volume. La 65 sovrascrive la prima)
- Prima di eliminare un volume su cui sono abilitate le Shadows Copie, ricordarsi di eliminare lo schedale relativo per evitare di avere messaggi di errori relativi all'impossibilità di portare a termine l'evento (Event ID 7001)
- Usare unità di allocazione di 16Kb o più quando si prepara un disco su cui si pensa di abilitare le Shadow Copies. Questo evita che un eventuale deframmentazione del disco provochi una cancellazione delle Shadow Copies

[↩ Inizio pagina](#)

Configurazione del client

Per poter visualizzare le versioni precedenti dei file, salvate con le Shadow Copies, è necessario installare sui client di rete il **Previous Versions Client**.

Il file di installazione del Previous Versions Client è disponibile, su qualsiasi server Windows Server 2003, nella cartella **C:\WINDOWS\system32\clients\twclient\x86**.

Per installarlo manualmente basta fare doppio click sul file **twcli32.msi**.

Non viene richiesta nessuna attività e in pochi secondi l'installazione terminerà.

In un dominio Active Directory è possibile installare il Previous Version Client creando una Group Policy di distribuzione del software.

[↩ Inizio pagina](#)

Funzionamento

Ora che abbiamo terminato la parte di configurazione, analizziamo il funzionamento delle Shadow Copies.

In fase di abilitazione delle Shadow Copies è stata eseguita una prima fotografia dello stato dei cluster del disco E:.

Da un client, accediamo ora allo share di rete **\\FB-DC01\DatiUtenti** e apriamo il file Documento-1.doc. Il suo contenuto è semplicemente:

Documento 1 – originale

Aggiungiamo al documento la riga
Versione 1

e salviamolo. Il documento conterrà ora il testo
Documento 1 – originale
Versione 1

Sempre dallo share di rete facciamo click con il tasto destro del mouse e sul file Documento-1.doc e, dal menù contestuale, scegliamo l'opzione **Properties**.

Nella finestra di dialogo **Documento-1.doc Properties** selezioniamo il tab **Previous Versions**.

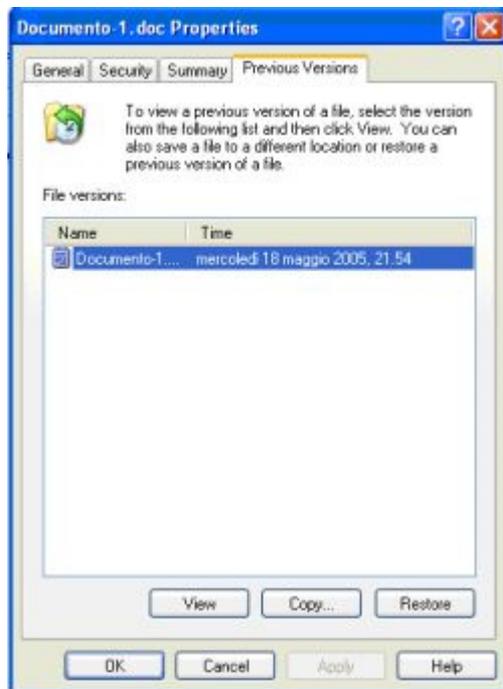


Figura 10.

Nella lista **File Versions** è presente la versione originale del file appena modificato. Abbiamo a disposizione tre bottoni:

- **View:** consente di aprire in sola lettura la versione di file selezionata
- **Copy:** consente di ripristinare il file originario come copia della nuova versione, in un percorso a scelta, anche diverso da quello originario
- **Restore:** ripristina il file nella sua posizione originaria sovrascrivendo la nuova versione che viene persa.

Cliccando sul bottone **View** posso vedere il contenuto originario del file Documento-1.doc:

Documento 1 – originale

Chiudiamo la finestra di dialogo **Documento-1.doc Properties**

Aggiungiamo al nostro file una nuova riga, contenente il testo *Versione 2*, e salviamolo. *Il file Documento-1.doc contiene ora il seguente testo:*

Documento 1 – originale

Versione 1

Versione 2

Riaprendo le proprietà del file Documento-1.doc e selezionando il tab Previous Version vediamo che continua ad essere presente una sola versione salvata del file. Aprendola si nota immediatamente che è la versione originale. Abbiamo perso la versione uno del documento, contenente il testo:

Documento 1 – originale

Versione 1

Questo avviene perché tra la prima e la seconda modifica non sono state eseguite Shadow Copies.

Proviamo ora ad eseguire manualmente una Shadow Copy.

Per fare questo dobbiamo andare sul file server, aprire le proprietà del disco E:, selezionare il tab **Shadows Copies** e cliccare sul bottone **Create now**. Non è necessario avvisare i nostri utenti di chiudere i file che stanno modificando: possiamo eseguire questa operazione anche mentre i file sono aperti!

Ora torniamo sul client e al file Documento-1.doc, accedendovi via share, aggiungiamo la riga:

Versione 3

In modo che il file contenga ora questo testo

Documento 1 – originale

Versione 1

Versione 2

Versione 3

Salviamolo e, sempre accedendovi via share di rete, apriamone le proprietà.

Il tab **Shadows Copies** contiene ora due versioni del file (figura 11).

La prima (quella più in basso nella lista) è la versione originale del file contenente il testo:

Documento 1 – originale

La seconda (quella più in alto nella lista) è la versione due contenente il testo:

Documento 1 – originale

Versione 1

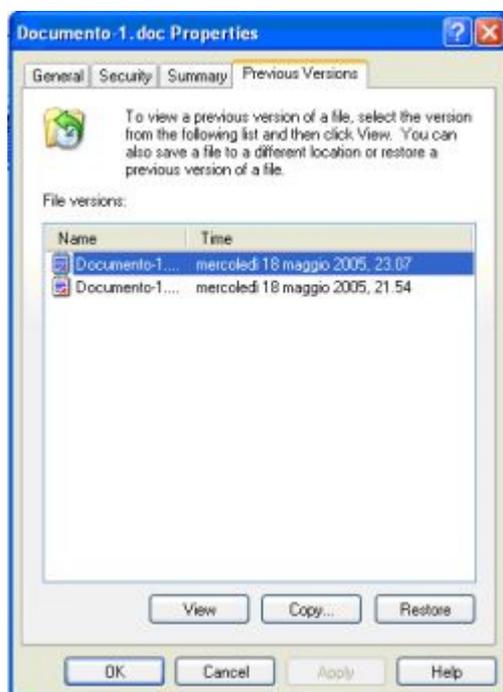


Figura 11.

Cosa succede se cancelliamo il file Documento-1.doc?

È possibile recuperarlo?

La risposta è sì. Vediamo come.

Dallo share di rete \\FB-DC01\DatiUtenti cancelliamo il file Documento-1.doc; dopo averlo cancellato, clicchiamo con il tasto destro del mouse in una zona libera della finestra dello share di rete e, dal menù contestuale, scegliamo la voce **Properties**. Nella finestra di dialogo **DatiUtenti on FB-DC01 Properties** scegliamo il tab **Previous Versions**.

Come è possibile vedere in figura 11, esistono versioni precedenti per l'intero folder.

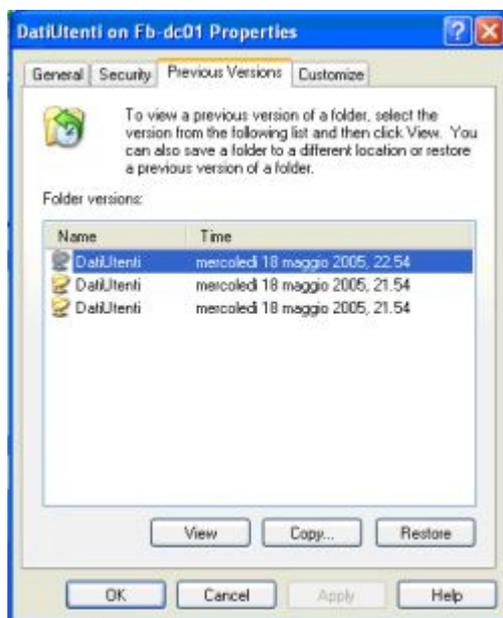


Figura 12.

Selezioniamo la versione più recente (la prima in alto nella lista) e clicchiamo il bottone **View**.

Si aprirà una nuova finestra che rappresenta la versione salvata dell'intero folder. All'interno di questa finestra (la cui caption è nel mio caso **DatiUtenti on Fb.dc01 (mercoledì 18 maggio 2005, 22.54)**) comparirà magicamente il nostro documento cancellato (figura 12). Un semplice drag-and-drop del documento ci consente di ripristinare il documento cancellato.



Figura 13.

[↕ Inizio pagina](#)

Conclusioni

Le Shadow Copies costituiscono un ottimo strumento che, al costo di un po' di spazio su disco, consente agli utenti della nostra rete, in molti casi, di recuperare da soli i file erroneamente cancellati o sovrascritti.

Si deve ovviamente fornire loro un minimo di istruzione iniziale e convincerli ad usare gli share di rete per salvare i propri documenti.

Resta un'ultima cosa da sottolineare: le Shadow Copies of Shared Folders NON sostituiscono i normali backup, che devono essere sempre e comunque eseguiti con regolarità.

Le shadow Copies sono uno strumento integrato dei backup e non un loro sostituto

[↕ Inizio pagina](#)

Link correlati

- [Windows Server 2003](http://www.microsoft.com/italy/windowsserver2003) [<http://www.microsoft.com/italy/windowsserver2003>]

[↕ Inizio pagina](#)