



## Peerlock erleichtert Arbeit mit DFS

# Windows im Gleichklang

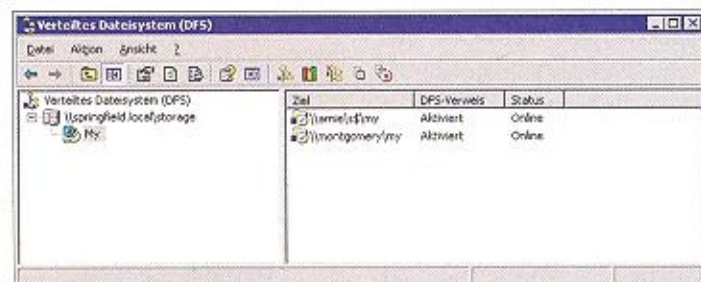
Es gilt, mehrere Dateien und Ordner in verteilten Netzwerken mittels einer Replikation unter Einsatz des Distributed-File-Systems (DFS) von Windows synchron zu halten. Doch was zunächst einfach klingt, kann schnell zu einem Problem werden. Die fehlende Funktion der Dateisperre für Replikationspartner will die hier vorgestellte Lösung nachliefern.

Das amerikanische Unternehmen Peer ist nach eigenen Angaben mit über 15 Jahren Markterfahrungen spezialisiert auf die Themen Backup, Replikation, Collaboration und auf eine tiefgreifenden Versionskonfliktkontrolle im Windows-Umfeld. Mit einer ganzen Reihe von Produkten für verschiedene Szenarien in unterschiedlich großen Umgebungen bietet der Hersteller aus New York alle Variationen, die sich aus dem „Gleichhalten eines Ordnerinhalts“ ableiten lassen. Im Portfolio finden sich spezielle Lösungen für ein Backup von Laptops, die ihre Datenbestände automatisch bei einer Internet-Verbindung in Richtung des eigenen Desktop-PCs oder eines Servers übermitteln. Zudem bietet der Hersteller auch Collaboration-Varianten für CAD-Systeme an, bei denen bekanntlich sehr große Dateien entstehen, oder die Sicherungen von Datenbanken, Exchange-Installationen oder die Übertragung von virtuellen Servern über das Netzwerk. Ei-

ne kleine Erweiterung für das weitverbreitete DFS von Microsoft bietet der Hersteller unter dem Namen „Peerlock“ an. Der Test sollte aufdecken, an welcher Stelle diese Software in einem „normalen“ Windows-System eingreift.

### Der Standard: Vorteile und Grenzen von DFS

Das Distributed File System (DFS) der Microsoft-Win-



**Bild 1.** Die Situation auf dem Windows-Server: Sobald ein Zweig im Distributed-File-System von mehr als einem Server als Replikat geführt wird, können Probleme bei der Synchronisation der Informationen auftreten.

dos-Server ermöglicht eine Abstraktion der Datenspeicherbereiche, die dabei losgelöst von den eigentlichen Server-Namen arbeitet. Eine reguläre

Freigabe, die über einen UNC-Pfad angesprochen wird (beispielsweise \\servername\freigabename) ist bei einer Veränderung des Server-Namens automatisch ungültig, sofern der Name nicht über die Namensauflösung „künstlich“ am Leben gehalten wird. Was in kleinen Unternehmen durch eine zwar lästige, aber durchaus machbare Anpassung der Zugriffe manuell zu erledigen ist, führt in größeren Unternehmen zum Fiasko. Das DFS wird vom Betriebssystem als logische Struktur über verschiedene Server gelegt, die entsprechenden Speicherplatz anbieten. Die Zugriffe der Client-Systeme erfolgen dann nicht mehr auf die Freigabe eines Servers, sondern werden vom System mithilfe des abstrahierten Namens im DFS durchgeführt. Das DFS stellt auf diese Weise eine Art „virtuelles File-System“ zur Verfügung.

Der besondere Vorteil dieser Technik liegt darin, dass ein Systemverwalter das DFS in einem verteilten Netzwerk einrichten und es dann mithilfe des Microsoft-Replikationsdienstes (File Replication Service –

möglichen es so, dass die Zugriffe der Client-Systeme auf die Server möglichst schnell ablaufen.

Eine Word-Datei, die in einem solchen DFS-Verbund gespeichert wird, steht automatisch an mehreren (n) Standorten zur Verfügung. So müssen die Anwender die entsprechenden Dateien auch nicht mehr per E-Mail im eigenen Unternehmen verschicken.

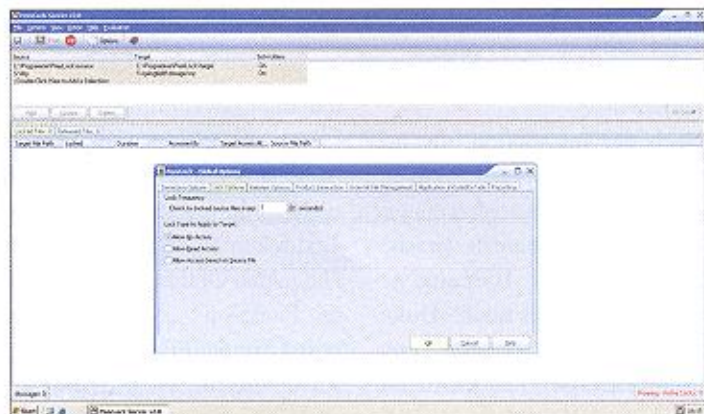
### Die Rolle des Domänen-Controllers

Jeder Administrator, der über mehr als einen Domänen-Controller in seinem Netzwerk verfügt, hat die File-Replikation bereits in Aktion erlebt. Die Replikation des SYSVOL-Verzeichnisses der DCs setzt diesen Dienst für diese Aufgabe ein. Anmeldeskripte oder Gruppenrichtliniendateien werden über diesen Weg auf allen Domänen-Controller stets identisch gehalten.

Es handelt sich sowohl bei den Anmeldeskripten als auch bei den GP-Dateien um sehr kleine Files, die sich selbst bei Verbindungen mit schmaler Bandbreite zügig austauschen lassen. Größere Dokumente, wie die bereits erwähnten CAD-Dateien, sind über diesen einfachen Replikationsdienst kaum zu transportieren. Erst der Windows Server 2003 in der R2-Ausprägung wurde nachträglich um einen neuen Replikationsdienst erweitert. Anstelle die kompletten Dateien immer wieder aufs Neue zu kopieren, ist das DFSr des R2 über die Technik Remote Differential Compression (RDC) in der Lage, bei diesen Vorgängen lediglich die Änderungen an einer Datei zu übermitteln.

Wenn also beispielsweise ein Anwender ein 5 MByte großes Word-Dokument editiert, und er dabei lediglich die Überschrift ändert, so ist der Stan-

tioniert der FRS von Windows problemlos. RDC arbeitet nach einem gänzlich anderen Verfahren: Die im DFS zu replizierenden Dateien sind in kleine Stü-



**Bild 2.** Der andere Ansatz: Die getestete Software erweitert die Standardfunktionen von Windows um die Fähigkeit, Dateisperren auch Replikationspartnern innerhalb von Sekunden mitzuteilen.

dard FRS von Windows gezwungen, auch in diesem Fall die komplette Datei zu übermitteln. Mit Hilfe von RDC werden beim DFSr lediglich die wenigen Bytes der geänderten Überschrift übertragen. So verringert sich dank RDC die Übertragungsdauer von einigen Minuten auf wenige Sekunden. Die SYSVOL-Replikation der Domänen-Controller des Windows Server 2003 R2 verbleibt jedoch beim einfachen FRS ohne RDC. Mit der Einführung des Windows Server 2008 steht der verbesserte Replikationsdienst nun auch aber für das SYSVOL-Verzeichnis zur Verfügung.

Technisch betrachtet arbeitet FRS mit einem Trigger und einem kleinen Cache-Pufferspeicher. Schließt das Betriebssystem eine Datei, so wird diese in den Cache-Speicher übertragen. Wird diese Datei dann für mehr als drei Sekunden nicht verändert, so beginnt die Replikation an alle angeschlossenen Partner. Mit wenig veränderten und kleinen Dokumenten funk-

cke (so genannte Chunks) unterteilt, die dann bei Veränderung übermittelt werden.

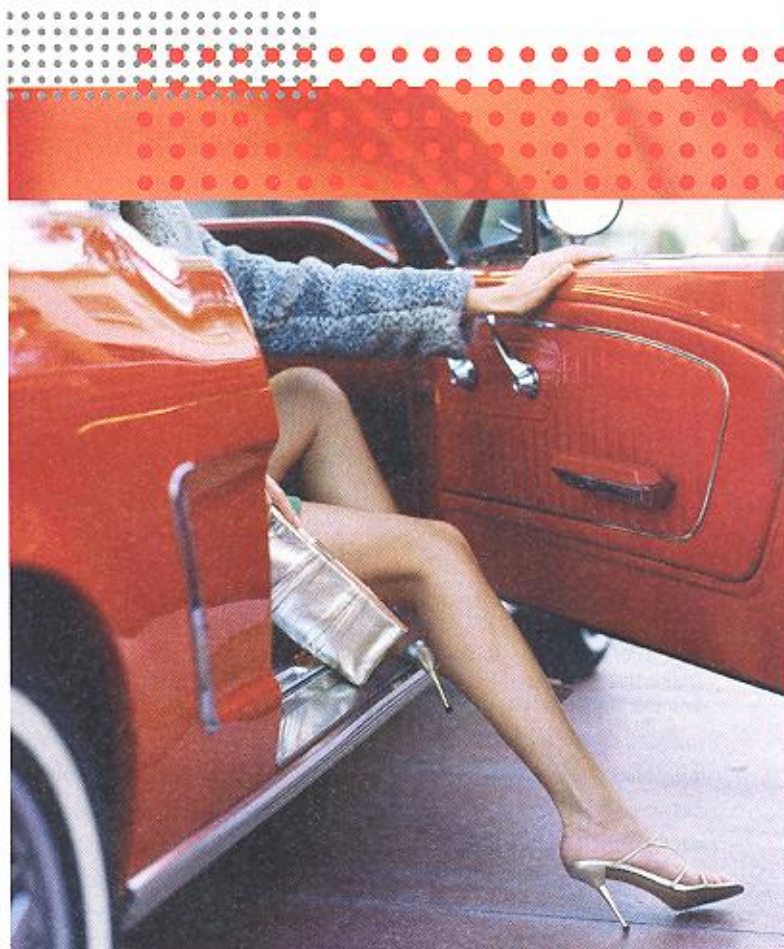
#### Probleme beim Einsatz der Standardlösung

Die ersten Erfahrungen mit der Replikation machen IT-Abteilungen typischerweise mit einem zentralisierten Backup von Dateien von Außenstandorten. Anstelle Mitarbeiter in kleinen Dependancen das regelmäßige Wechseln von Sicherungsmedien aufzubürden, werden die Dateien vornehmlich in der Nacht zur Zentrale repliziert und dort gesichert.

Die positiven Erfahrungen führen häufig dazu, dass ein DFS bereitgestellt wird, in dem alle Dateien aus allen Standorten über die Replikation gespiegelt zur Verfügung stehen. Da Microsoft in den Replikationsmechanismus jedoch keine Sperrvorrichtung eingebaut hat, kann es zu folgendem Szenario kommen: Am Standort A öffnet ein Mitarbeiter ein Excel-Dokument und ändert eine

## Steigen Sie ein ...

Alcatel-Lucent



und nutzen Sie unser umfangreiches Partner-Programm für **Data-/Voice-Reseller** mit bis zu 7% zusätzlicher Marge, kostenlosen Sales- und Postsales-Schulungen sowie Leads für Ihr Unternehmen.

Mehr Infos finden Sie unter [www.alcatel-lucent.de](http://www.alcatel-lucent.de) und bei unserem Value-Added Distributor KOMSA SYSTEMS.

BIS ZU  
7%  
EXTRA-MARGE



**Komsa**  
**SYSTEMS**  
DATA VOICE NETWORKING

[www.komsa-systems.de](http://www.komsa-systems.de)  
Mirko Eisele  
Tel.: 0 37 22/7 13-600  
[systempartner@komsa.de](mailto:systempartner@komsa.de)

Information in dem Dokument. Gleichzeitig öffnet am Standort B ein anderer Mitarbeiter dieselbe Datei und ändert ebenfalls Informationen in diesem Dokument. Der Mitarbeiter an Standort A speichert das Dokument, und anschließend speichert auch der Mitarbeiter an Standort B die Excel-Datei. Einzig die Variante von Standort B bleibt erhalten – da diese das

dass es zu Inkonsistenzen der Replikate kommt.

Exakt an dieser Stelle greift die lediglich 20 MByte umfassende Software Peerlock ein und fügt dem DFS eine Dateisperre hinzu. So soll die Problematik der überschriebenen Replikatsversionen überhaupt nicht entstehen können. Die Software erweitert das DFS mit dem FRS um die Fähigkeit, geöffnete Da-

Installation verwendeten wir die 15-Tage Testversion, die der Hersteller über das Internet kostenfrei anbietet. Die Konfiguration erfordert die Installation auf mindestens zwei Servern, die über DFS und FRS einen identischen Stand an Daten vorhalten.

Nach der Installation, die nur wenige Augenblicke dauert, findet sich im Startmenü ein mit dem Programmnamen versehener neuer Zweig. Hier sind neben einigen „Lies mich“-Dokumenten eine komplette, englischsprachige Dokumentation und die Konfigurationssoftware zu finden. Die ebenfalls komplett in Englisch gehaltene Konfigurationssoftware besteht lediglich aus sechs Registern und einer zusätzlichen Optionsmaske.

Die administrative Hauptaufgabe besteht darin, die lokale Variante eines Verzeichnisses, die so genannte „Source“-Quelle, mit der entfernten Variante auf dem Replikationspartner, die hier als Target bezeichnet wird, zu verbinden. Peerlock unterstützt sowohl die Eingabe von UNC-Pfaden als auch den Abgleich über Netzwerklaufwerksbuchstaben.

### Domänenübergreifender Abgleich

Ist ein domänenübergreifender Abgleich nötig, so muss der Administrator die Zugriffsdaten in Form von Benutzernamen und Passwort eingeben, ganz so, als ob er ein Netzwerklaufwerk verbinden will. In der Summe erlaubt es die Software einem Server bis zu 255 Source/Target-Paare zu verwenden, die eine beliebig große Anzahl von Unterordnern besitzen dürfen.

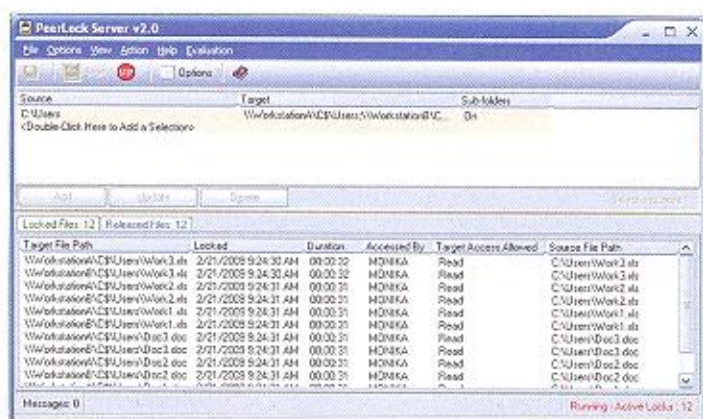
Das Optionsmenü der Lösung bietet eine große Anzahl von Parametern, über die das Locking sehr fein gesteuert werden kann. Der Anwender kann die Replikationssperre für einzelne Dateien aber auch für ganze Dateiartern über die Dateinamenerweiterung deaktivieren. Allerdings funktioniert diese Locking zum Beispiel nicht mit einfachen ASCII-Textdokumenten.

Die in den Optionen aktivierbare Funktion „Allow Access based Source Files“ bietet dem Anwender die Möglichkeit, eine Datei nicht generell für den Zugriff zu sperren, sondern sie den Replikationspartnern für die Dauer des Lockings im „Nur-Lese-Modus“ anzubieten. Selbst eine zusätzliche Cache-Funktion für einen schnelleren Zugriff bietet die Software, die auch mit einer Dateisperre versehen ist.

### Fazit: Mängel bei DFS/FRS beseitigt

Das Distributed File System (DFS) in Kombination mit dem File Replication Services (FRS) ist eine einfache Möglichkeit, Dateien an verschiedenen Standorten vorzuhalten, schnelle Zugriffe zu ermöglichen und den Aufruf möglichst einfach zu halten. Durch den Einsatz von Peerlock werden die systembedingten Mängel im Microsoft-DFS/FRS-Gespann beseitigt. Es versteht sich von selbst, dass Peer seine eigene Synchronisationssoftware „Peersync“ als deutlich leistungsfähiger favorisiert.

Thomas Bär/Frank-Michael Schleder/jos



**Bild 3.** Welche Dateien wurden wann, wie und durch wen gesperrt? Diese Informationen kann der Administrator anhand der Oberfläche und der Reports leicht ermitteln.

jüngere Datum aufweist. Die „etwas ältere“ Datei von Standort A wird gemäß der Konfliktbewältigung unbenannt und in einen dafür vorgesehenen Konfliktordner für gelöschte Dokumente überführt. Ein Eintrag in der „ConflictandDeletedManifest.xml“-Datei ist dann gewissermaßen ein letztes Lebenszeichen dieser Datei.

### Ein wichtiger Punkt: Die Lösung sperrt Dateien

In der Standardeinstellung ist der Konfliktordner auf eine Quota von 660 MByte eingestellt und beginnt automatisch mit dem Löschen von Dateien ab einer Auslastung von 90 Prozent. Je mehr Standorte in einem DFS mit Replikation zusammengefasst sind, desto höher ist die Wahrscheinlichkeit,

teien gegenüber einem weiteren FRS-Partner als gesperrt anzuzeigen. Ist eine Datei X auf dem Server A bereits geöffnet, so lässt sie sich innerhalb von Sekunden nicht mehr auf Server B öffnen.

Die Einrichtung und Installation der Software hat im Test keinerlei Probleme bereitet: Vor dem Download der Software wird der Anwender explizit gefragt, in welcher Systemumgebung Peerlock eingesetzt werden soll. Die Standard-Version ist für Windows 2000, XP und 2003 vorgesehen. Eine spezielle Variante für Windows Vista und Windows Server 2008 ist für die Zusammenarbeit mit dem UAC (User Account Control) optimiert. Mit den x64-Editionen von Windows arbeitet die Software problemlos zusammen. Zur