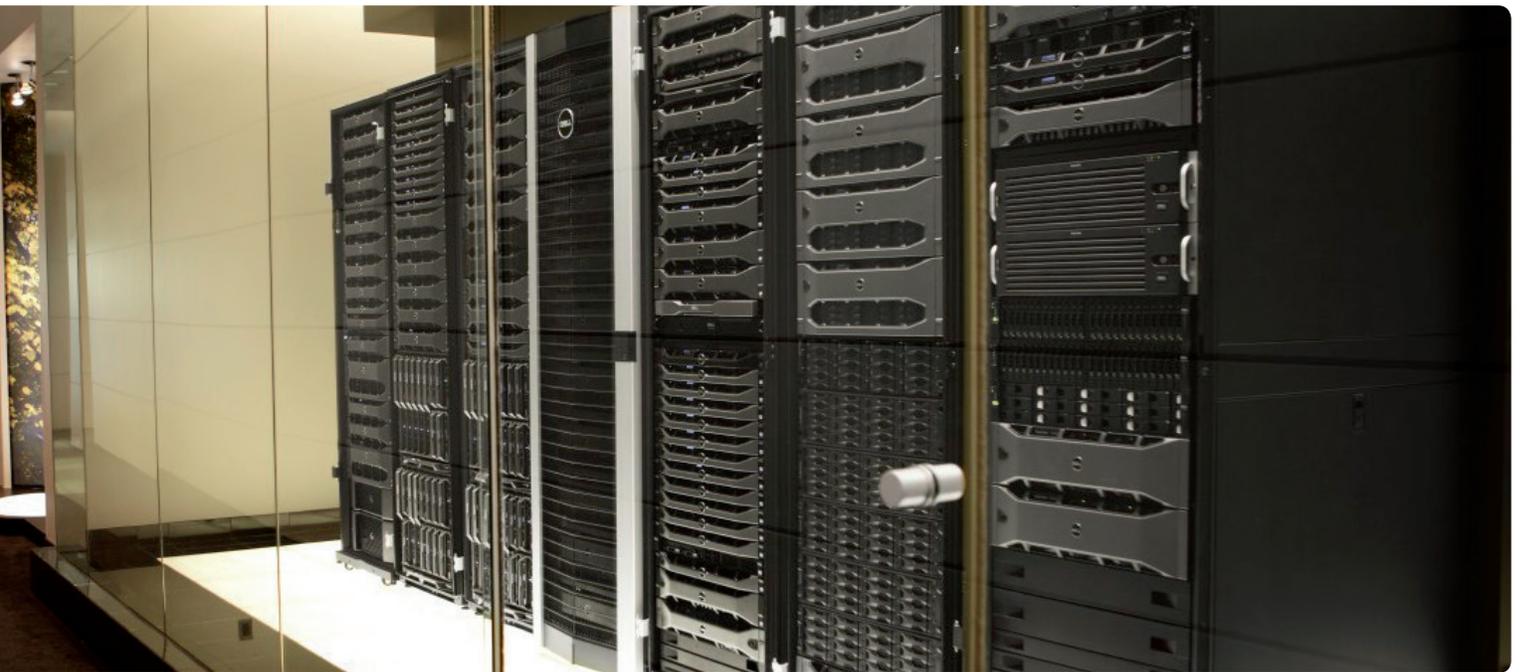


File server migration

The pain is in the permissions



Abstract

Moving all of a file server's files to a new server with permissions intact—whether to consolidate several file servers into one, or because you need to move files to a virtualized file server—is a pretty awful process. You can't drag and drop files from one server to another with Windows Explorer; it would take far too long for everything to copy. And while it seems like you should be able to simply back up the files from the old server and restore them to the new server, that approach often doesn't work, either. This paper explains why, and then explores how to find the right tools for the job to ensure migrated data retains the same file securities, permissions, shared folder rules and local group configurations as before

Introduction

The task: moving files to a new server while maintaining permissions

Ever had to move all of a file server's files to a new server? Perhaps in order to consolidate several file servers into one, or maybe because you needed to move the files to a virtualized file server? It's a pretty awful process, isn't it?

Windows Explorer just doesn't cut it. You're not going to drag and drop files from one server to another, because it'll take nine hundred million years for everything to copy. Most administrators probably rely on the good old tape backup approach: Back up the files from the old server, and restore them to the new server.

But it doesn't always work. While modern backup and recovery solutions are perfectly capable of restoring permissions along with files, it isn't always that simple.

Permissions get out of control really quickly. It takes only one little exception, which nobody will remember to document, for things to start breaking down.

The challenges

Permissions exceptions: so easily out of control

Yes, I know, you assign permissions on files and folders only to domain groups. Both the old and new servers are in the same domain, so the SIDs on the files' Access Control Lists (ACLs) will work on either server. Right?

See, the thing is, permissions get out of control really quickly. It takes only one little exception, which nobody will remember to document, for things to start breaking down. A domain user SID winds up on an ACL. A local user SID winds up on an ACL. Now you're in for it, because that SID won't exist on the destination server.

Files you don't have access to

Worse are those files which, for some reason, you as the administrator have no permission to. Like all those so-precious files in Human Resources' departmental folder. Or the files that are locked, like all of those annoying Access databases, because users just will not close out their applications when they go home at night. You're not going to get those files on your tape backup, and they're going to prove to be the exceptions that you spend the rest of the weekend sorting through.

Files that need to be moved across domains

Heaven help you if you're moving files across domains. Now you'll also have to make sure groups are properly migrated first, and what about the groups that you want to rename or something? This could be the migration that never ends, or at least never ends well.

Too many (undocumented) groups

The last problem? If you're really, really careful about assigning permissions only to groups, you probably have, like, three million groups. Every little unique set of permissions that needs to be applied results in a new group. You start off with the "Sales" group, but then you're quickly creating the "Sales—Inside" and "Sales—

Outside" groups. Before long there are "Sales Managers" and "New Salespeople," along with "Sales—Major Products" and "Sales—Retail." If you didn't start documenting them early on, then you've got a zillion groups and nobody can remember exactly which permissions each one is for. You might as well just be assigning permissions to individual users for all the trouble you've "saved." We try to use domain groups as roles for a role-based access control (RBAC) system, but groups just don't exactly fill that need.

The consequences

These problems can become especially annoying when you're trying to move files in large batches, such as migrating to a new file server or moving files into a virtual file server. You wind up just perpetuating the permissions problem. Worse, if you find yourself moving files across domain boundaries, you end up with orphaned entries on access control lists (ACLs), accounts that don't match up in the source and destination domains, and other thorny issues. But these problems are all solvable.

Fixing the problem

Step 1: Report

The first step is to identify potential problems before you even start the migration. A reporting product can help. Point it at the old server and have it find files with permissions assigned to problematic groups, like local users or domain groups that won't be present on the destination server. In other words, let the computer do the repetitive, time-consuming work of figuring out what permissions are there. Boring and repetitive work is why we invented computers!

You're going to need a reporting solution that's well designed for this task, though. Your servers probably have hundreds of thousands of files, so just running a single-threaded PowerShell script isn't going to turn up the right results in anything less than a century. Look for an advanced, multi-threaded architecture

that can scan file and folder ACLs lightning-fast, so you'll have your report quickly. You can then re-permission the problematic files, remove local user accounts, replace domain groups, or do whatever you might need to get your data into the best shape possible for a migration. See if the tool has reports specifically designed to find local user and local group permissions.

This is also a good time to correct the sins of the past: If your organization is firm on assigning permissions only to domain group accounts (always a good idea), let that security scanner go and find all of the individual user permissions. Once it's dug them out, you can create the necessary user groups, put those users into them, and then re-permission the files.

Ideally, you'll want this to all happen inside a single, intuitive graphical console—you don't want to be constructing `icacls` command-lines or messing with scripts. Not that command-line tools or scripts are bad, but for a task this sizable, they're just not efficient enough. For a task this complex, you'll spend more time writing the scripts and constructing command lines than actually solving a problem!

Step 2: Ditch the tapes

Tape backups might seem like an obvious way to grab a whole mess of files and transport them to a new home, but migration via tape does have its limitations.

For one, it's difficult to ensure that permissions are correctly re-populated. Now, what you can do is restore the files from tape, and then use a security tool to back up just the permissions from the original server, restoring those permissions to the new server. But there's always the potential for one or more ACL entries to be invalid in the new location, especially if your migration is crossing domain boundaries.

Tape recovery also can't be scheduled. Sure, you can kick it off and go home for the night, but it's more difficult to conduct a phased migration where you move a chunk of files over to a new server each evening.

Tape recovery also won't address shared folders and their permissions, which can be especially troublesome when you're migrating a file server that contains user home folders. You'll end up having to manually re-create and re-permission the shares, and that's just painful. Other settings, such as file compression or encryption, may not migrate properly during a tape restore (depending on your recovery software) and that'll be more manual effort.

And there are always those files to which you, the administrator, don't have access, or which are locked by an open process.

Choosing the right tool

Key features

The solution is to use a tool designed specifically for data migration. We're not talking about Robocopy here, useful as that is, because it just doesn't have the intelligence we need to solve all of these issues. The tool will need to transfer files and folders, maintaining their original NTFS permissions, and also transfer local users, local groups, and even shared folders. You should be able to schedule migrations to run during maintenance windows, so that it's easy to conduct a phased migration by simply setting up the paths you want to migrate on whatever schedule you like. During a phased migration, the right tool can even permit the old server to remain in use, if it's capable of synchronizing the target server's contents with the original source.

This file migration tool will also need the ability to override "access denied" for administrators, ensuring that you get every single file. And for locked files, make sure it can be configured to

The solution is to use a tool designed specifically for data migration... The tool will need to transfer files and folders, maintaining their original NTFS permissions, and also transfer local users, local groups, and even shared folders.

You'll want a tool that creates a complete, detailed log of every action, enabling you to review migrations (even ones that happened when you were at home in bed) and deal with any exceptions that remain.

intelligently retry files before just giving up. It should also deal with encrypted files, offering an option to migrate the contents unencrypted if encryption fails on the destination server.

The right tool will offer options that tape restores don't, including the ability to map folders and files. Ever want to completely re-structure the folder hierarchy on a file server? A migration is a great opportunity to do so, and an intelligent file copy tool would make it straightforward.

Many applications rely on file attributes like "last accessed date" to manage things like change control; restoring files from a tape backup will often reset these and other attributes. Again, with the right tool you're in control: You could synchronize these attributes with the original data, ensuring that the new file server looks exactly like the old one.

And what about permissions to users and groups—especially local ones—that don't exist in the destination? Choose a tool that can apply intelligence to those local users and groups, either migrating them or intelligently remapping permissions as you direct.

Finally, you'll want a tool that creates a complete, detailed log of every action, enabling you to review migrations (even ones that happened when you were at home in bed) and deal with any exceptions that remain. Need to perform complex remappings of user and group accounts? This can often be needed when moving files between domains, and it's where a security scanner tool can help by performing ACL pairing. Imagine telling the tool which source users match which destination users (or groups), and letting it take care of the rest, migrating and remapping permissions from the old server to the new.

That security scanner could also help with post-migration cleanup by identifying orphaned SIDs on the new server and helping to clean up any SID History permissions on your files and folders. You should even be able to use it to perform a post-migration comparison of files' original permissions and their current ones, so that you can be assured that the correct permissions are in place.

Summary

We've constructed quite a wish list here, so let's review. We want to make it easy to fix problematic file permissions, clean up those individual user permissions, and securely migrate files from place to place even in the largest, most complex environments. The capabilities fall into three types of tools: a "reporter," a "security scanner," and a "file migrator."

The "reporter" and "security scanner" are the tools designed to deal with ACLs and permissions on files. Together they need to be able to:

- Quickly scan file permissions—even on massive numbers of files—and report on them
- Have a multi-threaded architecture to run quickly across massive numbers of files
- Identify individual user permissions and replace them
- Remap user groups after a file migration, fixing permissions
- Clean up SID History and identify orphaned SIDs
- Compare permissions on two sets of files
- Run without scripting—using a graphical user interface instead

That handles the permissions side of things. To complete the task, the "file migration" tool will need to be able to do the following:

- Quickly copy files while retaining their ACLs
- Intelligently retry locked and open files

- Schedule batches of files to be copied whenever you want
- Create detailed log files of every action
- Inventory and copy shared folders, and their permissions
- Re-structure folder hierarchies on the fly while maintaining permissions
- Retain file compression and encryption attributes
- Retain—or set—file date, archived, and other attributes
- Synchronize files between two locations to enable a phased migration
- Create local users and groups as needed to maintain permissions
- Create post-migration reports to ensure files were copied correctly

Where can you get all of these capabilities?

The Dell Solution

A 1-2-3 punch for intelligent file migration

Three Dell products will do it all: Enterprise Security Reporter, Security Explorer and Secure Copy:

- Enterprise Security Reporter is the “security reporter,” identifying permissions that are

incorrect or no longer needed.

- Security Explorer is the “security scanner and repair robot,” scanning for problems and letting you fix them in batches.
- Secure Copy is the “intelligent file migration tool,” offering all of the features above to make any kind of batch file copy operation secure, easy, and reliable.

Together, these three solutions provide a powerful combination for migrating files and folders, including their permissions, in a wide variety of scenarios—including difficult, cross-domain migrations.

Learn more about these products by visiting:

- Enterprise Security Reporter: www.quest.com/enterprisesecurityreporter
- Security Explorer: www.quest.com/security-explorer
- Secure Copy: www.quest.com/secure-copy

All three are available as a free trial, so give them a spin and see for yourself how easy migrating files can be.



For More Information:

© 2012 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT,

DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com

Refer to our Web site for regional and international office information.

