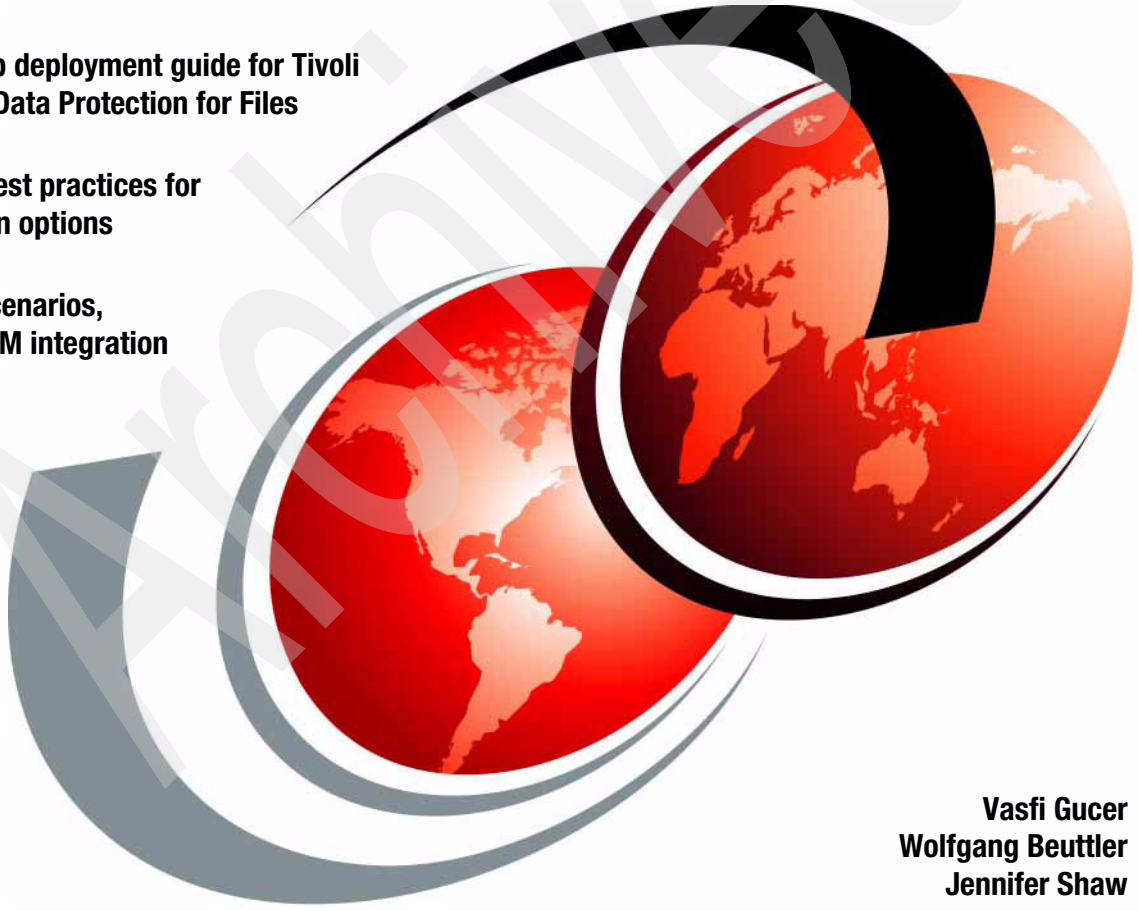
Tivoli software

IBM

Deployment Guide Series: Tivoli Continuous Data Protection for Files

- Step-by-step deployment guide for Tivoli Continuous Data Protection for Files
- Discusses best practices for configuration options
- User case scenarios, including TSM integration



Vasfi Gucer
Wolfgang Beuttler
Jennifer Shaw

Redbooks

ibm.com/redbooks

International Technical Support Organization

Deployment Guide Series: Tivoli Continuous Data Protection for Files

May 2006

SG24-7235-00

Note: Before using this information and the product it supports, read the information in “Notices” on page xiii.

First Edition (May 2006)

This edition applies to IBM Tivoli Continuous Data Protection for Files Version 2.1 (program number 5608-APF).

Contents

Figures vii

Tables xi

Notices xiii
Trademarks xiv

Preface xv
The team that wrote this redbook. xv
Become a published author xvi
Comments welcome. xvii

Chapter 1. Introduction to Tivoli Continuous Data Protection for Files . . . 1
1.1 General overview of Tivoli Continuous Data Protection for Files 2
1.1.1 What is Tivoli Continuous Data Protection for Files? 2
1.1.2 Why Tivoli Continuous Data Protection for Files is needed 4
1.1.3 Who should use Tivoli Continuous Data Protection for Files? 6
1.1.4 Tivoli Continuous Data Protection for Files and the IBM TotalStorage Open Software Family 8
1.2 How Tivoli Continuous Data Protection for Files works. 9
1.3 Main features of Tivoli Continuous Data Protection for Files 12
1.4 Value proposition of Tivoli Continuous Data Protection for Files 13
1.4.1 Benefits of using Tivoli Continuous Data Protection for Files 15
1.4.2 Unique differentiators 15

Chapter 2. Product architecture, planning, and deployment 17
2.1 Product architecture 18
2.1.1 Main components 18
2.1.2 Capabilities 18
2.1.3 Directories and files. 20
2.1.4 Daemon architecture. 22
2.1.5 IBM Tivoli Storage Manager integration 25
2.2 Planning for deployment 26
2.2.1 What are my critical files? 26
2.2.2 Do I need scheduled backup?. 27
2.2.3 Where should I back my files up to? 27
2.2.4 How often do I need to back up different types of files? 28
2.2.5 Do I need the Vault feature? 28
2.3 Deployment 29

2.3.1 Installation 29
2.3.2 Configuration 30
2.3.3 Advanced configuration 38
2.4 Using Tivoli Continuous Data Protection for Files 43
2.4.1 Restoring files 43
2.4.2 Status 46
2.4.3 Activity 48
2.4.4 Reports 50

Chapter 3. Troubleshooting, hints, and tips 51
3.1 Installation issues 53
3.1.1 Disk space 53
3.1.2 Non-privileged users 54
3.1.3 Port conflicts 55
3.2 Replication problems 67
3.2.1 Removable disk issues 68
3.2.2 File server issues 72
3.3 IBM Tivoli Storage Manager issues 75
3.3.1 Missing IBM Tivoli Storage Manager client options file (dsm.opt) . . . 78
3.3.2 Passwordaccess generate versus passwordaccess prompt 82
3.3.3 IBM Tivoli Storage Manager client option Subdir Yes not valid 93
3.3.4 Conflicting include/exclude lists 95
3.3.5 Files containing named streams (Alternate Data Streams) 98
3.4 Log files and FPcommand.bat 108
3.4.1 Tivoli Continuous Data Protection for Files logs 109
3.4.2 IBM Tivoli Storage Manager specific log files 111
3.4.3 File FPcommand.bat 113
3.5 Tracing 115

Chapter 4. Use case scenarios 121
4.1 Using Tivoli Continuous Data Protection for Files in a single-user environment 122
4.1.1 Single computer with no network connection 122
4.1.2 Single computer with an ISP connection 124
4.2 Multiple computers in a home or small business 124
4.3 Multiple users in a large enterprise environment 126
4.3.1 Tivoli Continuous Data Protection for Files on a file server 126
4.3.2 Distributed installation of Tivoli Continuous Data Protection for Files . . 128
4.4 Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager working together 131
4.4.1 Overview 132
4.4.2 Details 135

4.4.3 Summary 171

Chapter 5. Frequently asked questions 173
5.1 Include, exclude, and file lists 174
5.2 Replication features 175
5.3 File versions 176
5.4 IBM Tivoli Storage Manager (TSM) 177
5.5 Network operations 178
5.6 Removable disks 179
5.7 Miscellaneous 179

Chapter 6. Upcoming features 183
6.1 Translation 184
6.2 Encryption 185
6.3 Web-based Distributed Authoring and Versioning (WebDAV) 185
6.4 Improved user interface 186
6.5 Compression 187
6.6 Integration with TSM API 188

Related publications 189
Publications 189
Online resources 189
How to get IBM Redbooks 189
Help from IBM 190

Index 191

Figures

1-1 Why Tivoli Continuous Data Protection for Files is needed 6
1-2 Tivoli Continuous Data Protection for Files and the IBM TotalStorage Open Software Family 8
1-3 Unique hybrid approach of Tivoli Continuous Data Protection for Files. . 9
1-4 General overview of Tivoli Continuous Data Protection for Files 10
2-1 Agent-driver interaction 20
2-2 Replication threads 25
2-3 Configure continuous protection window 31
2-4 Configure scheduled protection window 33
2-5 Configure exclusions window. 35
2-6 Synchronize window 37
2-7 Vault window 39
2-8 Advanced settings window. 41
2-9 Restore window 44
2-10 Status window 46
2-11 Current Activity window 48
2-12 Reports window 50
3-1 Installation summary window 53
3-2 Insufficient disk space warning window 54
3-3 Error window due to write-protected installation director 55
3-4 Another program already using port 9003 56
3-5 The Tivoli Continuous Data Protection for Files reporting a problem . . 57
3-6 Tivoli Continuous Data Protection for Files entries in the event log. . . . 58
3-7 Error entry in the Windows system event log. 59
3-8 Port number in the FpPort DWORD Value 60
3-9 Modifying the FpPort DWORD Value. 61
3-10 Changing the port number to 9005 61
3-11 New port number in the FpPort DWORD Value. 62
3-12 The original start.html file with port 9003 63
3-13 The start.html file after editing (now using port 9005) 63
3-14 Netstat -a output showing the usage of the new port 9005 65
3-15 Successful entry in the Windows system event log 66
3-16 The Tivoli Continuous Data Protection for Files GUI using port 9005 . . 67
3-17 External USB disk named USB_Drive mapped as drive F: 68
3-18 Drive F: (USB_Drive) as remote backup target 69
3-19 Disk full informational message 69
3-20 Remote Space Configuration settings 70
3-21 Changed drive letter assignments 71

3-22 Informational message that the network target cannot be reached 72
3-23 Remote location is reachable again and replication continues 74
3-24 Shared network folder e$ on file server Izmir mapped to drive (W:) . . . 74
3-25 Using the UNC name instead of the drive letter. 75
3-26 The dsm.opt file as used in our lab 78
3-27 Continuous protection using the TSM every five minutes 79
3-28 Error “ANS1035S Options file dsm.opt not found” in the event log 80
3-29 FilePath error entry in the system event log 81
3-30 Contents of the files TSMout.log and TSMout.log_acp (ANS1035S) . . 81
3-31 Pending activities for the IBM Tivoli Storage Manager 83
3-32 The TSM Backup/Archive client process dsmc.exe in the Windows Task Manager. 84
3-33 Ending the dsmc.exe process 85
3-34 Warning message when terminating the dsmc.exe process 85
3-35 The Tivoli Continuous Data Protection for Files information message . 86
3-36 “TSM failed to process any data” error entry in the system event log . . 86
3-37 Informational message in the system event log due to connection problems with the TSM server. 87
3-38 File dsm.opt without the PASSWORDAccess option. 87
3-39 File dsm.opt with PASSWORDAccess generate option 88
3-40 TSM Backup/Archive command-line client session 90
3-41 TSM Backup/Archive client GUI. 91
3-42 Successful communication with the TSM server 91
3-43 The number of files protected by the TSM. 92
3-44 File dsm.opt using the SUbdir Yes option 93
3-45 Entry in the dsmserror.log due to SUbdir Yes being used in dsm.opt . . 94
3-46 Example of a minimum exclude list for the TSM Backup/Archive client. 96
3-47 File dsm.opt with exclude statement for *.xls files 96
3-48 ANS1115W warning message in dsmerror.log (excluded file). 97
3-49 Content (STREAMCONTENT) of a named stream (STREAMNAME). . 99
3-50 Messages ANS1228E, ANS4005E, ANS1804E in the dsmerror.log . . 100
3-51 Content of the filelist TSMAuditFile-active.log_3_select_acp 100
3-52 The TSM Backup/Archive command-line client console output with error messages. 102
3-53 Error messages ANS1345E in the dsmerror.log 103
3-54 No error messages in the console output (TSMout.log_acp). 104
3-55 Logging on to the TSM server using the TSM command-line client . . 105
3-56 The TSM server activity log with session 1292 (expire session) 106
3-57 The TSM server activity log with session 1293 (backup session) 107
3-58 Files to expire on the Tivoli Storage Manager server (TSMAuditFile-active.log_4_expire_acp). 108
3-59 TSMAuditFile-active.log_3_select_acp 108
3-60 FPcommand.bat when using TSM for continuous data protection . . . 114

3-61 FPcommand.bat when using TSM for continuous data protection . . . 114
3-62 FPcommand.bat when using TSM for scheduled data protection 114
3-63 FPcommand.bat when using TSM for scheduled data protection 115
3-64 FilePath agent in interactive mode. 118
3-65 Command to start a Tivoli Continuous Data Protection for Files trace 118
3-66 Create file.doc to trigger an activity 118
3-67 DebugView capturing the trace output. 119
3-68 Command to stop the trace 119
3-69 Quitting the interactive mode of the FilePath agent. 119
4-1 Home or small office configuration. 125
4-2 Simple deployment of Tivoli Continuous Data Protection for Files in a large environment 127
4-3 Distributed deployment of Tivoli Continuous Data Protection for Files in a large environment 129
4-4 Overview about the computer environment of XYZ, Inc. 133
4-5 ITSO lab setup representing the computer environment of XYZ, Inc. . 137
4-6 Continuous (local and remote) configuration of the mobile computer Phoenix 138
4-7 Scheduled configuration (daily schedule) of the mobile computer Phoenix 139
4-8 Default exclusion list 140
4-9 Remote space configuration (advanced settings) of mobile computer Phoenix 141
4-10 Contents of internal drive D: (XP_DATA) and external USB drive G: (USB_Drive). 142
4-11 Continuous (local and remote) configuration of workstation Cairo . . . 144
4-12 Scheduled configuration (daily schedule) of workstation Cairo 145
4-13 Remote space configuration (advanced settings) of workstation Cairo 146
4-14 Windows Explorer showing the contents of internal drive D: (W2K3_DATA) and remote backup location on file server Izmir (\\izmir\e$) 147
4-15 Contents of shared drive E: (CDP_Data) on file server Izmir 151
4-16 TSM Client Acceptor Daemon (CAD) and TSM scheduler service . . . 160
6-1 Sample window from the new user interface design 187

Tables

1-1 Comparison between Tivoli Continuous Data Protection for Files and traditional backup solutions. 3
2-1 Summary of files in Tivoli Continuous Data Protection for Files 21
3-1 Example of the most important options of dsm.opt 77
3-2 Explanation of TSM Backup/Archive client option SUbdir 93
3-3 Installation log files. 109
3-4 Replication logs 110
3-5 Scheduled protection logs 110
3-6 Local pool log file and gendb 111
3-7 Log files when IBM Tivoli Storage Manager is used for continuous protection 112
3-8 Log files when IBM Tivoli Storage Manager is used for the scheduled protection 113
4-1 Explanation of TSM Backup/Archive client options DOMain and MANAGEDServices 153
4-2 Settings of copy group STANDARD in policy domains WORKSTATION and FILESERVER 161
4-3 Settings of TSM client schedule FS_DAILY_INCR 169

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM®	SANergy®	TotalStorage®
Redbooks™	Tivoli Enterprise™	
Redbooks (logo)  ™	Tivoli®	

The following terms are trademarks of other companies:

Excel, Microsoft, MSDN, Outlook, PowerPoint, Windows NT, Windows, Win32, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Tivoli® Continuous Data Protection for Files is specifically targeted at end user computers, such as mobile computers and workstations, as well as file servers. It provides continuous data protection of files, providing the highest level of protection possible, yet is simple to use and administer. When files change, Tivoli Continuous Data Protection for Files will make up to three copies of the file (or queue copies to be made later).

This IBM® Redbook presents a deployment guide for Tivoli Continuous Data Protection for Files. We cover planning, installing, and troubleshooting of Tivoli Continuous Data Protection for Files for several use case scenarios. In addition, we provide some case studies, including integration with IBM Tivoli Storage Manager, that can be used as a proof of concept or demonstration of the product at a client environment.

The target audience for this redbook is IT Specialists who will be working on Tivoli Continuous Data Protection for Files installations and proof of concepts.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

Vasfi Gucer is an IBM Certified Consultant IT Specialist at the ITSO Austin Center. He has been with IBM Turkey for 10 years, and has worked at the ITSO since January 1999. He has more than 13 years of experience in teaching and implementing systems management, networking hardware, and distributed platform software. He has worked on various Tivoli client projects as a Systems Architect and Consultant. Vasfi is also a Certified Tivoli Consultant.

Wolfgang Beuttler is an IBM Tivoli Storage Manager Support Specialist in Mainz, Germany. He works for the Tivoli Storage Manager front- and back-end support team and provides support to clients all over the world, including onsite support. He has more than 13 years of experience in IT and seven years of experience with IBM and the Tivoli Storage Manager product portfolio, starting with ADSM Version 3.1. His areas of expertise include defect as well as non-defect problem determination of Tivoli Storage Manager products.

Jennifer Shaw has worked for IBM since 2000. She started working in SQA for the Tivoli SANergy® software product. In 2002, she assisted the Tivoli SRM team as the Globalization test lead. Starting in 2003, she was involved in the design, project management, testing, and documentation of the FilePath project. In 2004, she was test lead for the System test phase of Tivoli SANM and by 2005 became the Installation test lead for the consolidated TPC product. Currently, she is working on globalization, documentation, and testing for Tivoli Continuous Data Protection for Files.

Thanks to the following people for their contributions to this project:

Arzu Gucer, Wade Wallace
International Technical Support Organization, Austin Center

Chris Stakutis, Jarrett Potts, Linda Sandmann, Pam Nesbitt
IBM USA

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners, and clients.

Your efforts will help increase product acceptance and client satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Discover more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. JN9B Building 905
  11501 Burnet Road
  Austin, Texas 78758-3493

1

Introduction to Tivoli Continuous Data Protection for Files

Tivoli Continuous Data Protection for Files is a new approach for backup and restore solutions by combining two technologies in a totally new and unique manner: *replication* and *traditional backups*.

Tivoli Continuous Data Protection for Files leads the current market direction in data protection by providing real-time protection for (highly important) files, being a to-disk solution, maintaining native file formats, and using a simplified file management concept.

This chapter provides an introduction to Tivoli Continuous Data Protection for Files and discusses the following topics:

- Introduction to Tivoli Continuous Data Protection for Files
- How Tivoli Continuous Data Protection for Files works
- Main features of Tivoli Continuous Data Protection for Files
- Value proposition of Tivoli Continuous Data Protection for Files

1.1 General overview of Tivoli Continuous Data Protection for Files

In today's on demand business environment, productivity is paramount and information is currency. Each day, gigabytes, or even terabytes, of new information will be produced or existing data changed in an average business environment. Some of the data is highly important and business critical, and some is maybe not that important and of less interest.

Data and information are the key factors for companies to drive their business. Therefore, companies need to protect their valuable and vulnerable assets against loss, corruption, or unwanted alteration.

Losing critical business information not only results in application outages, but can also lead to delays of important projects, diverted resources, or regulatory scrutiny. Overall, these points are associated with fairly high costs.

In many businesses, protection of data may also be required by law. This environment is driving IT managers to implement comprehensive solutions for managing the recoverability of enterprise data.

The solution for this situation is to ensure recoverability through the automated creation, tracking, and vaulting of reliable recovery points for all enterprise data.

And this is where Tivoli Continuous Data Protection for Files comes into play.

1.1.1 What is Tivoli Continuous Data Protection for Files?

Tivoli Continuous Data Protection for Files is a real-time, continuous data-protection solution for mobile computers, workstations, and personal computers. It is specifically designed to work well even if network connections are intermittent. But Tivoli Continuous Data Protection for Files also provides continuous protection for file servers, reducing or eliminating backup windows and the amount of data potentially lost in a failure.

Tivoli Continuous Data Protection for Files can back up your most important files the moment they change instead of waiting for a scheduled backup. Non-critical files are backed up periodically on a scheduled basis. It works in the background, much like a virus scanner, and is therefore totally transparent to the end user.

Since Tivoli Continuous Data Protection for Files has a single end-point architecture, there is no need for additional components, for example, a server component. It only requires a single installation on the system with files to be protected.

Tivoli Continuous Data Protection for Files keeps the protected instances of files in their natural format and does not modify them or encode them in a proprietary format. The advantage of maintaining files in their native format is that they are directly accessible and available by any application.

To protect files and make them available for date-based restore, Tivoli Continuous Data Protection for Files creates up to three separate copies of files:

- On local disk for protection, even when not connected to a network
- On a network file system for remote machine protection
- By using IBM Tivoli Storage Manager (TSM) for use in more sophisticated enterprises

Table 1-1 demonstrates the differences between Tivoli Continuous Data Protection for Files and traditional backup approaches.

Table 1-1 Comparison between Tivoli Continuous Data Protection for Files and traditional backup solutions

	Tivoli Continuous Data Protection for Files	**Traditional backup solutions**
When to protect	Continuous for highly important files, scheduled for others	Scheduled, full system
How to detect	Journal-based on *all* file systems	Journal-based on some file systems
Where copies are stored	Disk only, locally or remote; IBM Tivoli Storage Manager (TSM)	Typically on tape
Storage format	Left “native”, online as files	Wrapped into a proprietary format
Management / administration complexity	Simplified per-client administration only	Client-server concept; server component typically more expensive/complex

So overall, Tivoli Continuous Data Protection for Files provides simple, effective and real-time file protection for:

- Accidental file deletion
- File corruption
- Unwanted file alteration
- Disk crashes
- Other unforeseen disasters

1.1.2 Why Tivoli Continuous Data Protection for Files is needed

As already mentioned, driving a company's business is based on the availability of information and data. Though this should be enough to understand why it is mandatory to protect this data and information, there are several other facts that make this point even clearer:

- In many companies, about 60-70% of corporate data resides on desktops, mobile computers, and workstations, which are rarely backed up or not backed up at all.
- Almost half of the small and medium sized businesses admit to having no formal data protection procedure.
- Data growth is increasing rapidly.
- The loss of productivity due to data loss on endpoints is a growing concern.
- Virus and data corruption on file servers is an increasing problem.
  - Companies need better recovery point capabilities.
- Today's backup and recover solutions are difficult and tend to miss the most valuable data (what the user is working on now).
- Mobile computer/desktop data protection a growing problem:
  - Corporate data centers are reluctant to take on mobile computer management.
  - The business impact of lost data on mobile computers/desktops is increasing:
    - Specific segments, such as law firms, medical practices, consulting, and so on, can have a very significant impact to productivity and liability.
    - The aggregate impact to large corporations is significant.

With this in mind, Tivoli Continuous Data Protection for Files is designed to help alleviate clients' concerns and provide simple, effective, and efficient data protection and integrity. Key client issues driving the requirements for continuous data protection are:

- Critical information assets are being stored across the organization; they are no longer consolidated on just a few key servers.
- The complexity and expense associated with the replication of information assets across an organization.
- A shortage of skilled people resources, which demands that highly automated tools be deployed to help allow consistent practices across platforms, minimize human error, and improve the amount of storage a single storage administrator can handle.

- Meeting service-level objectives by providing continuous availability of data.
- The integrity of data for governance and security requirements.
- Backups made “only” on a daily basis allow too much productivity loss.

One of the current market trends is the steadily declining cost of disk storage (local hard drives, SAN disks, removable disks, NAS devices, and so on). This trend makes file protection using replication technologies more cost effective compared to traditional backup/recovery solutions, which mostly use tapes as their storage repository.

Tivoli Continuous Data Protection for Files anticipates this development through its unique approach as being a combination of both a traditional backup and recovery solution using modern data replication techniques. In the long term, this approach will not only lead to a better utilization of the available technical infrastructure and improved labor productivity, but also yield to positive monetary effects. For more information about the value proposition and the benefits of using Tivoli Continuous Data Protection for Files, refer to 1.4, “Value proposition of Tivoli Continuous Data Protection for Files” on page 13.

Figure 1-1 summarizes the key points of why Tivoli Continuous Data Protection for Files is needed in business environments these days.

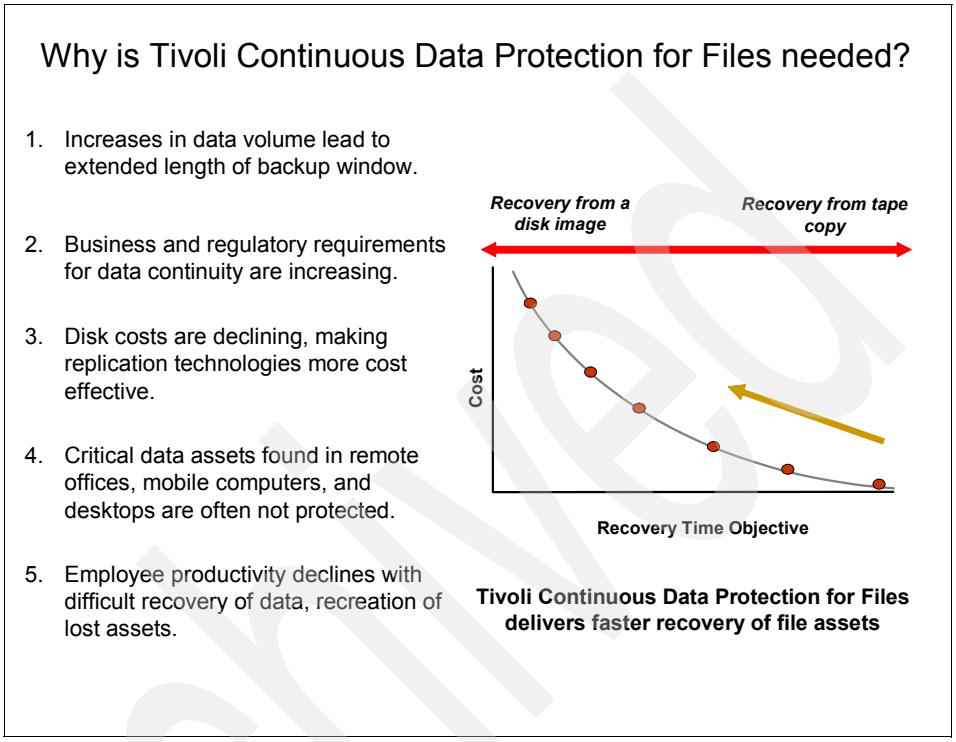


Figure 1-1 Why Tivoli Continuous Data Protection for Files is needed

1.1.3 Who should use Tivoli Continuous Data Protection for Files?

Due to the concept and design of Tivoli Continuous Data Protection for Files, it can be used to protect private mobile computers or personal computers at home as well as workstations or large file servers in business critical environments. Generally speaking, Tivoli Continuous Data Protection for Files *should be used by everyone* who has the need to continuously protect files in real time.

Anyhow, this section concentrates on business clients only, but most of the points mentioned here are also valid for individuals using Tivoli Continuous Data Protection for Files as their private data-protection solution at home.

Ideally, Tivoli Continuous Data Protection for Files can be used by organizations with multiple locations, departments, and file servers that have information assets used for client relationships and revenue activity necessary to the value and operation of the business.

Clients whose IT infrastructure includes desktops and mobile computers where information assets exist that are often not protected adequately or frequently are also a good candidate for using Tivoli Continuous Data Protection for Files.

Tivoli Continuous Data Protection for Files can also be of interest for enterprise clients with large file servers already using traditional backup solutions like IBM Tivoli Storage Manager (TSM) or VERITAS NetBackup. Due to the amount of data needed to be backed up, large file servers are often unable to meet their backup window. Tivoli Continuous Data Protection for Files can help by reducing or almost eliminating those backup windows and is therefore a perfect complement to traditional backup solutions.

Overall, Tivoli Continuous Data Protection for Files may be the answer when:

- Clients are considering buying disks as an alternative to tape for simpler administration and configuration and faster recovery service levels.
- Clients view data as a major corporate asset.
- Clients are considering snapshot technologies; with Tivoli Continuous Data Protection for Files, there is no need to understand more IT-savvy concepts such as “snapshots” and how maintain, configure, and age such elements.
- Clients are concerned about their ability to meet service and availability levels with a minimal to zero backup window.
- Skilled storage administrators are difficult to find or retain.
- Employee productivity suffers due to human errors causing data loss and lost time recreating data.
- Clients are considering a backup solution for remote offices

  Tivoli Continuous Data Protection for Files is ideal for remote office servers, as it will locally version and protect highly important files and migrate data back to corporate servers while tolerating network spottiness.
- System administrators need a centralized and automated way to protect the information residing on a mix of heterogeneous computers distributed throughout a network.
- System administrators need their computer systems to be online 24x7 with minimum CPU or network impact during data protection operations.
- The organization is considering how to easily protect information assets found on individual desktops, and mobile computers with minimum administration.
- The organization needs to protect critical files from alteration or deletion, viruses, and corruption

  Tivoli Continuous Data Protection for Files allows users to protect critical corporate assets by preventing deletion or alteration of active files by end users, viruses, or file corruption.

1.1.4 Tivoli Continuous Data Protection for Files and the IBM TotalStorage Open Software Family

Now that we know what Tivoli Continuous Data Protection for Files is used for and why it is needed, this section shows how Tivoli Continuous Data Protection for Files fits into the current IBM TotalStorage® Open Software Family. Figure 1-2 shows this in more detail.

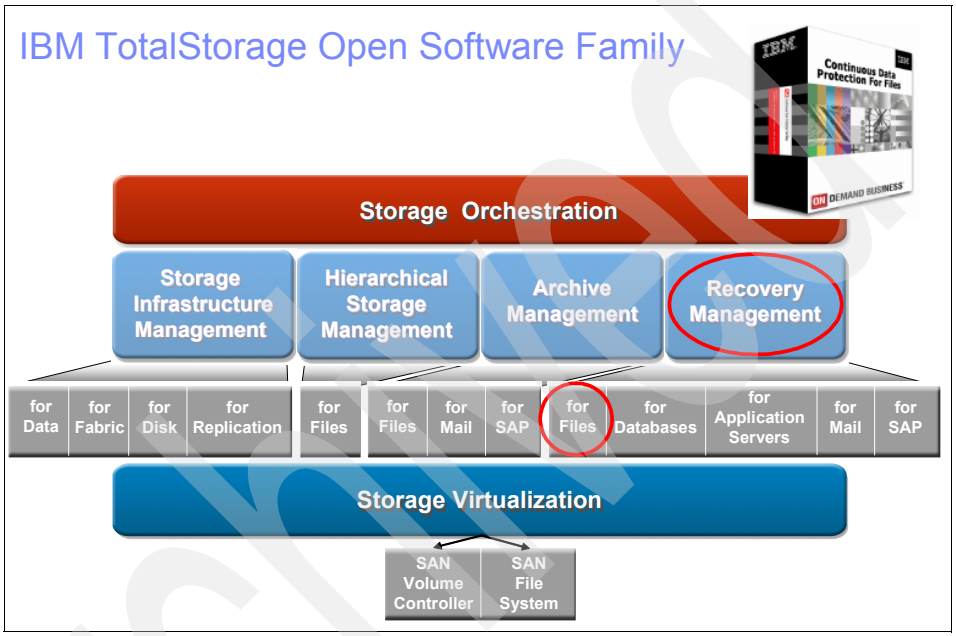


Figure 1-2 Tivoli Continuous Data Protection for Files and the IBM TotalStorage Open Software Family

Tivoli Continuous Data Protection for Files is part of the recovery management products of the IBM TotalStorage Open Software Family, and is specifically developed to be a real-time protection solution for files.

Others products belonging to the recovery management products category are, for example, IBM Tivoli Storage Manager for Databases, IBM Tivoli Storage Manager for Application Servers, or IBM Tivoli Storage Manager for Mail.

1.2 How Tivoli Continuous Data Protection for Files works

Tivoli Continuous Data Protection for Files is a new backup paradigm using a unique hybrid approach by combining modern replication technologies together with traditional backup methods. It does so by taking all the benefits from each technology and uniting them together into a completely new product: Tivoli Continuous Data Protection for Files.

Figure 1-3 shows this new paradigm as well as the benefits taken from both replication and traditional backup approaches.

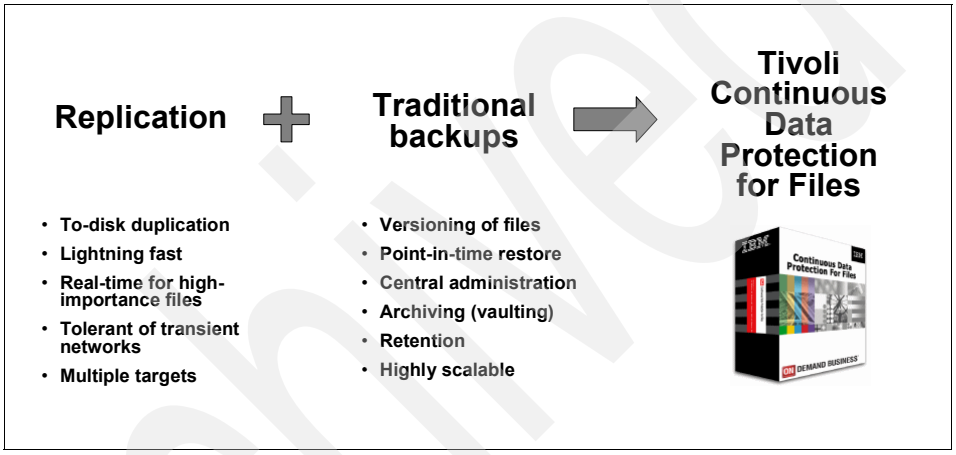


Figure 1-3 Unique hybrid approach of Tivoli Continuous Data Protection for Files

But how does it work? Figure 1-4 gives a general overview on how Tivoli Continuous Data Protection for Files works.

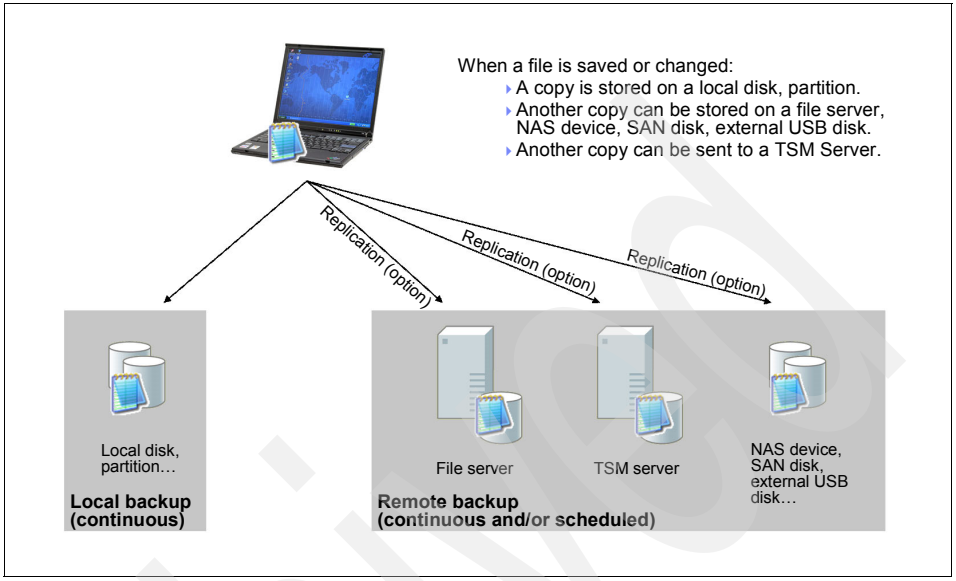


Figure 1-4 General overview of Tivoli Continuous Data Protection for Files

Whenever a file is changed or created, Tivoli Continuous Data Protection for Files notices it. If this file type is tagged as a high-priority continuous type (per the settings, such as a Microsoft® Word, PowerPoint®, Excel®, or other Office files), an immediate copy is made into a so-called backup area (a separate directory tree) on the local disk to avoid cluttering the natural location for the file. Tivoli Continuous Data Protection for Files will store many versions of each file (typically up to 20) subject to a “pool size” that can be configured. When the pool is full, the oldest copies (versions) are removed to make room for newer ones.

The same file can also be sent to a remote storage area, such as a file server, NAS device, SAN disk, and so on, for off-machine protection. If the remote file server is not currently available (perhaps due to not being in the network at the time), then the changed file is remembered and sent as soon as the network appears to be functioning. The files sent to the remote file server in this mode will have only a single instance stored (that is, not versioned), since they are versioned locally.

Another copy of the file can be sent to an IBM Tivoli Storage Manager (TSM) server, as Tivoli Continuous Data Protection for Files has special built-in support for TSM. Traditionally, TSM is a data protection product often used in larger business environments. Those clients might find Tivoli CDP for Files useful as a real-time client solution for mobile computers and workstations, yet still want

most of the protected data to ultimately be managed by a TSM server. To use this feature, a TSM client needs to be installed on the same system as Tivoli Continuous Data Protection for Files and a TSM server needs to be available in the network.

If scheduled protection has been enabled, then all other “non-important” changing files will be noticed by Tivoli Continuous Data Protection for Files and queued for transmission to the remote file server based on the interval that has been selected. When the interval expires, Tivoli Continuous Data Protection for Files will copy all of the changed files to the remote file server, or wait if the file server is not currently available.

All those types of protection offered by Tivoli Continuous Data Protection for Files (continuous or scheduled, local or remote) can be easily configured by the end user in any combination. This allows the user to protect his assets in a highly flexible manner.

To summarize how Tivoli Continuous Data Protection for Files works, we have to differentiate between high-priority (important) and all other files:

- High-priority files:
  - Specify up to three target areas for high priority files.
  - The target area(s) will capture every save of a file when it occurs.
  - The local target area is auto-managed as a pool with a configurable size.
  - Old versions are deleted to make room for new versions.
  - The local area allows untethered restores.
  - There is an option to specify a remote file server for off-machine protection; it is still real-time, but tolerant of being disconnected.
  - There is an option to specify a IBM Tivoli Storage Manager (TSM) server for off-machine protection; it is still real-time, but tolerant of being disconnected.
- All other files:
  - All other files are protected on a periodic basis by being sent to the remote file server or IBM Tivoli Storage Manager (TSM) server.
  - Change-journal eliminates having to take processor resources to scan the file system.
  - Files are “versioned” on a remote file server, allowing for point-in-time restore.
  - Remote versions are automatically managed to a configurable pool size.

1.3 Main features of Tivoli Continuous Data Protection for Files

While writing this redbook, the current version of Tivoli Continuous Data Protection for Files was Version 2.1. The main features of this version are:

- Continuous protection of important files without doing a thing.
- When a file is saved:
  - A copy is stored on local disk.
  - Another copy can be sent to a file server, NAS device, SAN disk, and so on.
  - Another copy can be sent to an IBM Tivoli Storage Manager (TSM) server
- Real-time data protection.
- High/low priority files options

  Tivoli Continuous Data Protection for Files allows high important files to be backed up continuously as soon as they change. Less important files can be saved on a periodic (scheduled) basis, for example, once a day.
- File include/exclude options

  Tivoli Continuous Data Protection for Files offers the usage of include/exclude lists. By using them, the client can define precisely what type of files will be monitored for protection. On the other hand, he can also specify a list of files or directories that will be ignored by Tivoli Continuous Data Protection for Files and thus not backed up or vaulted.
- Tolerant of transient networks

  Tivoli Continuous Data Protection for Files is designed to work well even if network connections are intermittent. If a remote storage area like, for example, a file server is currently not reachable due to network problems, Tivoli Continuous Data Protection for Files will remember the changes made to the file and send it as soon as the network appears to be functioning again.
- Versioning of files.
- Point-in-time restore.
- Archive retention.
- Scalable.
- Small foot print

  Tivoli Continuous Data Protection for Files can be installed in a few minutes on a system and will only take about 43 MB of disk space.

- Simplified management / central administration

  Due to its simplified management concept, Tivoli Continuous Data Protection for Files provides a central administration interface that allows the end user to restore his own files fast and easy.
- No server component required.
- Maintain native file format

  Tivoli Continuous Data Protection for Files maintains files in their natural format and does not encode them in a proprietary format or modify them in any other way.
- Open architecture.

1.4 Value proposition of Tivoli Continuous Data Protection for Files

For business units dependent on data availability and rapid data recovery, Tivoli Continuous Data Protection for Files provides uniquely efficient and effective data protection to ensure business continuity, employee productivity, and integrity of information assets.

For storage managers and administrators responsible for protecting data while containing cost, Tivoli Continuous Data Protection for Files simplifies heterogeneous storage management and provides real options for an integrated data protection solution across all information assets.

Tivoli Continuous Data Protection for Files:

- Provides easy to use data protection and integrity, reducing the cost of training staff to use it.
- Improves employee productivity by providing real-time backups of data, so no matter when a failure occurs, the recovery can be to the latest version, not the last time a scheduled backup ran.
- Improves IT productivity and labor resource utilization because end users can more easily recover files without IT involvement.
- Improves network and bandwidth usage, as it is optimized to send data through network only when it is connected and most efficient with no user or IT manual intervention required.

The value proposition using Tivoli Continuous Data Protection for Files can be summarized as follows:

- Reduced or eliminated backup window
  - Improved backup resource utilization
  - Better return on investment (ROI) and total cost of ownership (TCO)

> **Note:** In finance, the return on investment (ROI)[a] or just return is a calculation used to determine whether a proposed investment is wise, and how well it will repay the investor. It is calculated as the ratio of the amount gained (taken as positive), or lost (taken as negative), relative to the basis.
>
> Total cost of ownership (TCO)[b] is a financial estimate designed to help consumers and enterprise managers assess direct and indirect costs related to the purchase of any capital investment, such as (but not limited to) computer software or hardware.

a. Definition taken from article “Return on investment”, found at:
http://en.wikipedia.org/wiki/Return_on_investment
b. Definition taken from article “Total cost of ownership”, found at:
http://en.wikipedia.org/wiki/Total_cost_of_ownership

- Improved recovery point objective (RPO)
  - Reduced loss of data
  - Improved productivity

> **Note:** The RPO can be thought of as the degree of difference between the active online data and the disaster recovery copy of that data. A RPO of zero would mean that the primary copy and the disaster recovery copy are in exact synchronization. A failure would result in zero loss of data.

- Improved recovery time objective (RTO)
  - User initiated restore, zero administration intervention
  - Optional recovery from disk (local or remote)

> **Note:** The RTO is the amount of time after a failure that someone is willing to spend before a given application or group of data is back up and available. A RTO of zero means that failures should cause zero disruption.

1.4.1 Benefits of using Tivoli Continuous Data Protection for Files

Using Tivoli Continuous Data Protection for Files has the following benefits:

- Simplified storage management may save IT and end-user labor.
- Continuous data protection provides data integrity when viruses and corruption attack systems.
- Reduces or eliminates backup windows.
- Optimizes integration to network and enterprise data protection solutions.
- Optimizes bandwidth and network transfer of data.
- Continuously protects versions of files to allow clients a choice of recovery points.
- Ability to write-protect data locally even when not connected in case of virus, corruption, logical error, or user error.
- Ability to send data to heterogeneous backup devices: disk, NAS, USB, local partition, and LUN from SAN.

1.4.2 Unique differentiators

The following unique differentiators of Tivoli Continuous Data Protection for Files have been identified:

- Fast time to deployment

  Tivoli Continuous Data Protection for Files can be installed, configured, and running by an end user in a few minutes as one, single back-end solution.

- Ease of daily use

  No need to understand more IT-savvy concepts such as "snapshots" and how to maintain, configure, and age such elements.

- Elimination or reduction of backup windows
- Backup-target flexibility

  Tivoli Continuous Data Protection for Files allows the target of the backup to be any type of modern disk-based storage device, be it a USB device, an enterprise storage array, a closed-architecture Network Attached Storage (NAS), such as NetApp or Snap, or another logical unit number (LUN) from the Storage Area Network (SAN).

- Easily integrates into traditional backup solutions

  Tivoli Continuous Data Protection for Files integrates naturally with IBM Tivoli Storage Manager (TSM) as well as the backup target device, which can be backed up by any off-the-shelf data protection package.

- Effective backup for remote systems and traveling users

  Unique ability to locally cache versions when working disconnected and re-synchronize with a file system or device when reconnected makes it ideal for the remote/mobile user.

- Effective backup for remote offices

  Tivoli Continuous Data Protection for Files is ideal for remote office servers as it will locally version and protect high-importance files and migrates data back to corporate servers while tolerating network spottiness.

- Simple backup for department solutions

  Anyone, even with low administrative skills, can add Tivoli Continuous Data Protection for Files to a department file server and now has real-time file protection (even if just locally).

- User productivity

  With Tivoli Continuous Data Protection for Files, you can be assured that there is no loss of productivity due to re-creation of lost work. Other backup/recovery solutions offer near continuous protection: once an hour, or once a day, which simply is not as effective as continuous data protection is.

- Automating manual process to protect *all* corporate assets

  Users do not need to save to corporate systems for data protection and audit purposes; Tivoli Continuous Data Protection for Files automatically protects all changes to files (even when not connected to the corporate network), and provides a version level audit trail for changes.

- Protect critical files from alteration or deletion, viruses, and corruption

  Tivoli Continuous Data Protection for Files allows users to set protections for critical corporate assets to prevent deletion or alteration of LIVE/active files from end-user error, a virus, or corruption.

2

Product architecture, planning, and deployment

This chapter discusses the architecture, planning considerations, and deployment of Tivoli Continuous Data Protection for Files and contains the following sections:

- Product architecture
- Planning for deployment
- Deployment
- Using Tivoli Continuous Data Protection for Files

2.1 Product architecture

Tivoli Continuous Data Protection for Files is a relatively simple product that has just enough controls and options to allow for a wide range of different configurations. At its core, the program operates at the kernel level of the operating system, monitoring all file operations. It keeps track of all pertinent activities and performs other operations based on the configuration. So, Tivoli Continuous Data Protection for Files knows when you open files, when you close them, and whether or not you have changed the file when you close it. When there is a change saved, this is noted and a new version of the file is replicated to one or more locations, either immediately, or at a later time.

The underlying technology was designed to be a general file system extension tool that can be presented to the end user in a variety of different formats, for different purposes. The current product, Tivoli Continuous Data Protection for Files, mostly exploits the function of “copy-on-close replication.”

2.1.1 Main components

The main components of Tivoli Continuous Data Protection for Files are:

- Kernel

  fp.sys[1]: This is the driver that loads when the computer boots up. It is located in \%WINDIR%\System32\Drivers.

- User
  - FilePathSrv.exe: This is the daemon, or process, that starts as a service (CDPforFilesSrv). If you are running in regular user mode, this service will stop right away until it has something to do. If you are running in service mode, the service will stay active. To run it from a command prompt, type **`filepathsrv -d`**. It is located in the Installation directory.
  - fpa.exe: This is the command line, interactive program that passes commands to the kernel. It can be used to set tracing levels. It is located in the Installation directory.

2.1.2 Capabilities

The kernel layer of the product performs a number of activities:

- Audit: Watches file activity, particularly noting files that are closed with new data.
- Write Once Read Many (WORM): Prevents I/O or any alteration to files.

[1] The underlying technology of Tivoli Continuous Data Protection for Files is called FilePath. “fp” is shorthand for FilePath. Some internal components are called fp or use fp as a prefix.

- Mirroring: Kernel-based I/O mirroring: Inactive in the current product.
- Replication: Notification of files that are replicated.

The kernel layer is based on a set of rules that set up the conditions under which certain activities, or actions, are performed. The rules and actions come pre-configured to make the product act as designed. When Tivoli Continuous Data Protection for Files performs a basic local backup of a file that has changed, the kernel is obeying a chained set of rules and actions. A basic chain includes:

Rule: When should the action occur? “On Open,” “On Write” or “On Close”.

Meta rules (optional): What conditions apply? For example, it does not fall under the exclusion list, and it matches *.ppt (or something from the inclusion list).

Action: What to do if the rules are true? Trigger a replication, block I/O to this file (Vault action).

All of the basic rule-action chains required for Tivoli Continuous Data Protection for Files to function properly are kept in XML format in the file fpa.txt.

Important: Do not edit the fpa.txt file. First, you might change something in one of the rule-action chains, which will cause the product to become unstable. Second, Tivoli Continuous Data Protection for Files updates the file from time to time, so you might lose some information by saving over necessary changes.

The daemon, or process, handles the following activities:

- Executing the replication, or copy-on-close
- Driving the scheduled protection
- Displaying updated information in the GUI

See Figure 2-1 for an illustration of the relationship between the kernel layer and the daemon or driver.

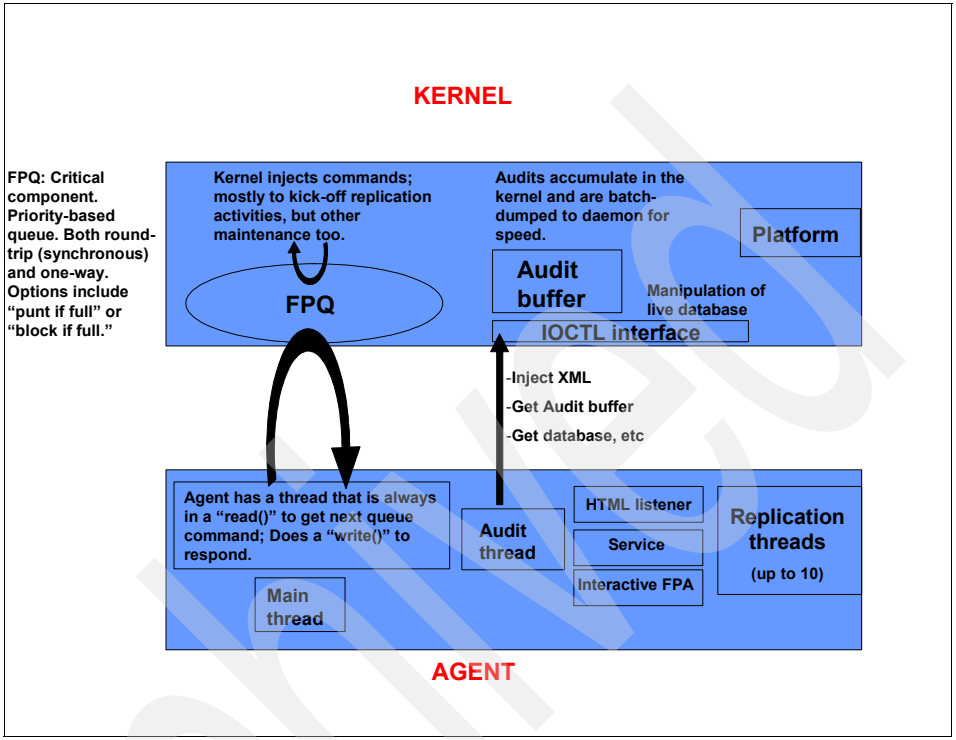


Figure 2-1 Agent-driver interaction

2.1.3 Directories and files

Tivoli Continuous Data Protection for Files uses a file-based architecture; it has no special or proprietary databases to hold files or keep track of the file activities it is monitoring. Instead, it uses the native file system and files as databases, including the generations database, which keeps track of file versions and changes.

See Table 2-1 for a description of the critical files in the product architecture.

Table 2-1 Summary of files in Tivoli Continuous Data Protection for Files

File/Folder name	Purpose
System Operation	
fp.sys	Main driver for the product.
FilePathSrv.exe	Daemon that monitors file activity in the kernel.
fpa.txt	A database where main “rules” and some configuration information is stored.
Replication	
replication.log	Contains the last 1.3 MB of replication transactions.
replication-queued.N[a]	Contains a list of the replication activities that are currently in the queue.
replication-active.N	Contains a list of the files currently being replicated.
replication-failed.N	Contains a list of the replication failures; this list is not limited by size and will continue to grow over the life of the product.
Scheduled Protection	
ChangeJournal.log	Contains a list of all the files pending for scheduled protection.
ChangeJournal.log_1_inprocess	Contains the instance that is currently being processed.
ChangeJournal.log_2_last	Lists the last file processed during scheduled protection.
ChangeJournal.log_LastSuccess	Holds the date and time of the last successful replication; this is reported in the GUI.
RemoteVersions.log	Holds an entry for each “versioned” file put at the target.
sysprotect_tsm_expire_out	Holds the output of the last batch sent to TSM.
purge_struggled.log	Lists the files that appear unreachable during a purge.

File/Folder name	Purpose
Local Pool	
LocalPool.log	List of all files currently in the local pool.
\gendb\	A directory tree that holds version names of files that have been replicated, along with the dates to facilitate purging the pool.
TSM (in the CDP mode)	
TSMAuditFile-queue.log	List of files currently accumulating for backup.
TSMAuditFile-active.log	List of files currently being sent to TSM.
TSMAuditFile-active.log_2_pack	List of files after duplicates have been removed.
TSMAuditFile-active.log_3_select	List of files sent to TSM for backup.
TSMAuditFile-active.log_4_expire	List of files sent to TSM for deletion.
TSMout.log	Last total output from TSM of both select and expire operations.

a. N refers to the priority given by the configuration to the different replication activities. If you have files being replicated at different priority levels, you will have multiple files; one for each priority level. See “Advanced settings” on page 40 for more information on priority levels.

2.1.4 Daemon architecture

The daemon runs several threads to perform its various functions. They are:

- Queue thread
- Audit thread
- Sysprotect
- TSM thread
- HTML listener
- Replication thread(s)

Queue thread

When the kernel needs something done that can only be done in user mode, it creates a “Queue” entry, posts it, and usually waits for a response from the daemon. The main daemon thread is the queue reader, which loops in a read(). There are about six commands that the queue thread may be asked to perform, but the most important one in this product is “Do a replication.” For each replication request at a given priority level, a file is opened and appended with

the specifics of the replication request. These files are in XML format. (See the Replication section of Table 2-1 on page 21 for a description of these files.) These files are monitored by the replication threads that are described below.

Audit thread

The main purpose for the audit thread is to wake up periodically and ask the kernel to dump its audit/log buffers. The audit buffers capture file change events that are used by Tivoli Continuous Data Protection for Files for scheduled protection and other activities. The daemon sleeps for a few seconds, and then drains any messages in the buffer (via an IOCTL request into the kernel). The buffer is formatted as a list of XML messages; each message indicates both the file to add this message to, and the message. The message can be anything defined by the “action,” and is typically in XML format itself. It includes various expanders (substitutions) for such things as filename, and so on. The following is an example of a message:

```
<change vfs=”Unlink” src=”C:\fp\buildchk.log” other=””size=”10697”
app=”System”/>
```

The ChangeJournal (sysprotect) rules/actions cause these audits to be accumulated into a file called ChangeJournal.log in the installation directory. The LocalPool rule causes audits to accumulate the locally versioned files into the LocalPool.log file.

Sysprotect

When this thread is started, its job is to perform a scheduled protection by addressing all of the files listed in the ChangeJournal.log file. This thread is started either on a periodic bases, or when the user selects **Backup Now** under the Scheduled Protection section of the Status window. When started, the thread will do the following:

1. Detect if the file ChangeJournal.log_1_inprocess exists, and process that file.
2. Automatically rename ChangeJournal.log to ChangeJournal.log_1_inprocess so that audits can continue to accumulate.
3. Process the ChangeJournal.log_1_inprocess file and record each line to the ChangeJournal.log_2_last file.

To minimize audit traffic, the kernel side keeps a hash of files that have been altered (tabulation) and avoids issuing multiple audits for files that have been repeatedly altered. This hash has a 2,000 file limit and then it cycles. Sysprotect also ignores the “vfs” mentioned in the log (see example message above) and determines what to do based on the current version of a file. For example, if the source file is missing, presume that an “unlink” should be performed.

The Sysprotect thread also performs the function of remote pool management. Every time a version is created on the remote target, an entry is made in the RemoteVersions.log file. The ServerPool metric is increased by the versioned file's size, and this metric is compared against the ServerPoolQuota metric that was configured in the Remote Space Configuration section of the Advanced Settings window in the Tivoli Continuous Data Protection for Files GUI. If the metric indicates that the pool size is over the quota, the following actions are performed:

1. The RemoteVersions.log file is consumed, one line at a time, deleting the oldest files and removing the file name from the list.
2. This continues until the pool size is at least 20% under the threshold size.
3. The remainder of the RemoteVersions.log file replaces itself.
4. Files deleted are logged as "unlinks" in the Replication.log file.
5. Deletions that fail are logged to either:
   - purge_failed.log: Generally when users have cleaned up the pool by deleting files themselves, in which case the pool size metric is decreased.
   - purge_struggled.log: Usually in the case of a network access type of error.

TSM thread

The TSM thread starts when a TSM backup occurs for the "real time" processing activity.

HTML listener

The HTML listener thread processes requests from the browser. The browser displays the product GUI, which has information about configuration and settings and is also used by the user to change configuration settings.

Replication thread(s)

The replication threads manage the replication activity. They are file-centric, and they monitor the replication files. The queue thread places the list of files to be replicated in a replication-queued.N file, where N is the priority. The replication thread automatically renames this to a replication-active.N file and then processes the replications in priority order. If the replication encounters a permanent failure, the transaction gets logged in the replication-failed.N file. All other transactions are posted to the replication.log file. These threads are restartable and persistent, which makes them easy to trace for diagnosing problems. Also, if the threads die, they will not stall the system. See Figure 2-2 on page 25 for a diagram of this process.

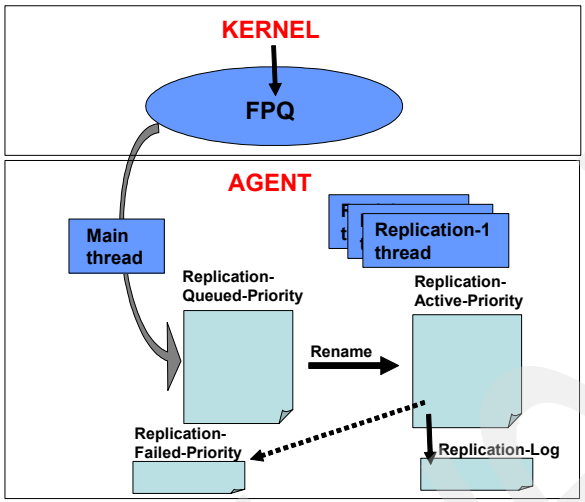


Figure 2-2 Replication threads

2.1.5 IBM Tivoli Storage Manager integration

Currently, Tivoli Continuous Data Protection for Files works with TSM in the following manner. You must have a TSM client set up on your system that is pointing to an active TSM server. If you choose to have your files backed up to a TSM server, either under Continuous or Scheduled protection, Tivoli Continuous Data Protection for Files will create and maintain a separate file list of files that have changed. See Table 2-1 on page 21 under the TSM section for a description of these files.

When the time interval for protection has been reached, Tivoli Continuous Data Protection for Files will pass the file list on to TSM using the TSM client command line. This command tells the server which files to back up. The files are selected using the Include/Exclude lists you have set up in Tivoli Continuous Data Protection for Files. However, the TSM server exclude list will be respected, so if your changed file is on the TSM exclude list, it will not be backed up to the TSM server. Just like regular remote replications, if you are not attached to the TSM server when the time interval is reached, Tivoli Continuous Data Protection for Files will wait and retry.

2.2 Planning for deployment

Although it is fairly simple to install and configure Tivoli Continuous Data Protection for Files, it is worth your while to spend a little time considering how to deploy the product so that you will get the most out of it. In this section, we will discuss general considerations to keep in mind as you install and configure the product. There is more detailed information in 2.3, “Deployment” on page 29. See Chapter 4, “Use case scenarios” on page 121 for more details on several use cases that describe how to implement the product in a larger environment, installing on multiple machines or file servers.

For a single machine installation, the most important consideration is to make sure that you have a window of time to configure the product so that it is working most efficiently for you. Tivoli Continuous Data Protection for Files is a “set it and forget it” type of product, so once you have it set up, it will run in the background and you will be mostly unaware of it until you need to restore a critical file. To make sure that you can easily restore the correct version of a file at that critical point, it is well worth spending a little time up front to review your configuration.

Before you begin, you should consider the following questions:

- What are my critical files?
- Do I need scheduled backup?
- Where should I back my files up to?
- How often do I need to back up different types of files?
- Do I need the Vault feature?

2.2.1 What are my critical files?

By default, Tivoli Continuous Data Protection for Files will back up the contents of your \My Documents\ folder, along with a few other file types (see 2.3.2, “Configuration” on page 30 for more details). If you typically save all of your critical documents under this directory path, then you will not need to add anything to the inclusion list. If, however, you save critical files in a different directory path, you should consider what type of files they are, and where they get saved. Some programs select a different path by default, or you may have set up a different location for some files. In this case, you need to consider where those files get saved and what type of files they are and what the file extension is. Depending on your situation, you will need to add either the directory path or the file extension to your inclusion list.

2.2.2 Do I need scheduled backup?

Tivoli Continuous Data Protection for Files also offers a more traditional form of backup that, by default, includes all files on your hard drive except for the files included in your Exclusion list. You can back up these files to either a remote server or your pre-configured TSM server. We highly recommend that you include scheduled backup as an option if it is possible in your environment for the following reasons:

- You may have missed some important file types in your inclusion list.
- You may install software that creates a new directory structure for saving files, and thus would not be caught by the inclusion list.
- There may be other files that get damaged or accidentally deleted that are important for the operation of various programs on your computer. Having these files backed up on some schedule may prevent you from having to reinstall software.

Important: The Scheduled Protection option offered in Tivoli Continuous Data Protection for Files cannot be used to do a complete system restore in the event of total hard drive failure. It does not take a complete "snapshot", including system files that would be required for a complete system restore.

2.2.3 Where should I back my files up to?

The default location for continuous data protection is to a local disk on your computer. Tivoli Continuous Data Protection for Files will automatically select the drive with the largest free space as the target location. The primary use of this backup site is for you to have immediate access to recently saved versions of your files. If you save a version of a file but need to "undo" that save, or if you mistakenly delete an important file, you can easily restore a previously saved version of the file from your local backup. If you are working on a computer that is not connected to a network, or any type of external storage, this will be your only backup location. If you have access to some sort of remote storage, you will probably want to consider one or more of the other backup options. These options include a local hard drive (local network or USB drive), a remote file server, and a remote TSM server. We highly recommend using the remote backup option if at all possible in the event that your hard drive fails or is lost. You will need to know the fully qualified UNC path for your remote drive to configure it properly. Check with your network administrator if you do not know what to use.

Tip: If you will be backing up several computers to a single network drive, you do not need to set up a separate folder for each user. Tivoli Continuous Data Protection for Files will create a unique folder for each computer with the computer's network name at the top of the directory structure, directly underneath the RealTimeBackup folder.

2.2.4 How often do I need to back up different types of files?

There is no easy answer to this question. The very best, but totally impractical, configuration would back up every version of every file and keep them forever. Since this is not possible, you need to think about what best suits your needs. If you are going to implement either the remote continuos option or the scheduled backup option, you will need to think about both the volume of your backup, as well as the timing of it.

Remote continuous

Although this backup option is labeled continuous, this is not always literally true. Tivoli Continuous Data Protection for Files makes note of all of your file saves, but if you are not currently connected to the network, or if you are in between the time intervals you have set up for TSM backups, a list of file changes will be kept to be backed up at the next possible time.

When you are selecting a time interval for TSM backups, keep in mind that the most recently saved version of a file will be sent when your TSM interval is due. That is, if you set your TSM interval for 30 minutes, and you save a file 10 times in that interval, only the last version of the file will be sent to your TSM server. The number of versions of that file kept in TSM is configured in TSM.

Although you do not explicitly set the time interval for continuous remote backups to a file server, you should keep in mind what percentage of time you are connected to the network. This will have an impact in the number of versions you select to keep on the remote target before they are eligible to be purged.

2.2.5 Do I need the Vault feature?

In some cases, you may have files that need to be preserved in their exact format for a period of time. One way to do this is to write them to a CD-ROM. However, with the Vault feature in Tivoli Continuous Data Protection for Files, you can protect these files in the same way. Once they are considered to be in the Vault, they cannot be changed in any way. They are available as read-only versions and cannot be altered or deleted. Some users may need this function for regulatory reasons. For example, if you are required to keep financial records in their original form for seven years, you can put these files in a directory covered under

the Vault function. Tivoli Continuous Data Protection for Files will protect them from editing and deletion.

2.3 Deployment

Now that you have thought a little bit about how you need to use Tivoli Continuous Data Protection for Files, you are ready to install the product. Remember, although it only takes a few minutes to install, especially if you keep the default configuration options, you should make sure that you have some time to fine-tune the configuration by reviewing how it is working after installation.

Tip: At the end of the installation, you have the option to synchronize your backup location(s). This will pre-seed your backup targets with your existing files. Although normal operation of Tivoli Continuous Data Protection for Files does not impact your computer operation, the Synchronize function can take up a significant amount of your computing resources and can take several hours to complete. Keep this in mind as you select a time for installation.

2.3.1 Installation

The installation can be performed using the following steps:

1. Double-click the Tivoli Continuous Data Protection for Files installer icon. InstallShield starts and displays the Language Selection dialog. Tivoli Continuous Data Protection for Files V.2.1.x is not translated, so you should accept the default English selection.
2. Click **OK**. The Tivoli Continuous Data Protection for Files Information window will display with the build number.
3. Click **Next**. The License Agreement window will display.
4. Read the License Agreement, and select the radio button to accept the terms.
5. Click **Next**. The Installation Location window will display.

Note: At this time, we advise you to use the default Installation location rather than changing to a different location.

6. Click **Next**. The Installation Confirmation window will display with the Installation options you have chosen.

7. Confirm that the information is correct and click **Next**. You will see a progress bar indicating the installation progress. You will also see a command prompt window open as the Installer runs several scripts. When the installation is complete, an Installation complete window will open in the background at the same time that the Tivoli Continuous Data Protection for Files GUI opens in a browser window so you can begin configuring the product right away.
8. After you are done configuring the product (see the 2.3.2, “Configuration” on page 30 for details), close the browser window and click **Finish**.

Although you do not technically have to go through the configuration windows to have Tivoli Continuous Data Protection for Files start protecting your files, we recommend that you at least review the default settings so you are aware of how things are set up. Then, let Tivoli Continuous Data Protection for Files run for a few days, complete the fine tuning (see “Fine tuning” on page 41), and then do the synchronization (see “Synchronize” on page 36).

2.3.2 Configuration

If you are sure that you do not need to change any of the settings from the default configuration, you can simply close the browser immediately and Tivoli Continuous Data Protection for Files will be running in the background. We recommend that you at least review the configuration so you are aware of the current settings. If you close the browser immediately, you will also not synchronize your backup and target locations. That is, every file you change from this point on will be protected under continuous protection, but files you changed previously will not be.

Recommended configuration

Although Tivoli Continuous Data Protection for Files is fairly easy to configure, there are a number of different options that allow for a wide range of different configurations. Here is a summary of the typical recommended configuration:

- Local Continuous backup: Enabled, 2 GB pool, includes MS Office file extensions and other user-created content that is considered high value.
- Remote Continuous backup: Disabled. It is usually unnecessary to add this load to the network; consider Scheduled, hourly if you really need good currency on the network target.
- TSM Continuous backup: Disabled. Again, it is usually unnecessary to add this load to the network, and it could cause an undesirable number of versions in the TSM database.
- Scheduled backup: Enabled, Daily. 10 GB pool (or approximately a sixth to a tenth the size of the source disks), five versions, broader inclusion list than local. Alternatively, set the inclusion to “*” and schedule a weekly backup.

Continuous protection

The first window you see during the initial setup of Tivoli Continuous Data Protection for Files is the Continuous protection configuration window for both Local and Remote protection (Figure 2-3).

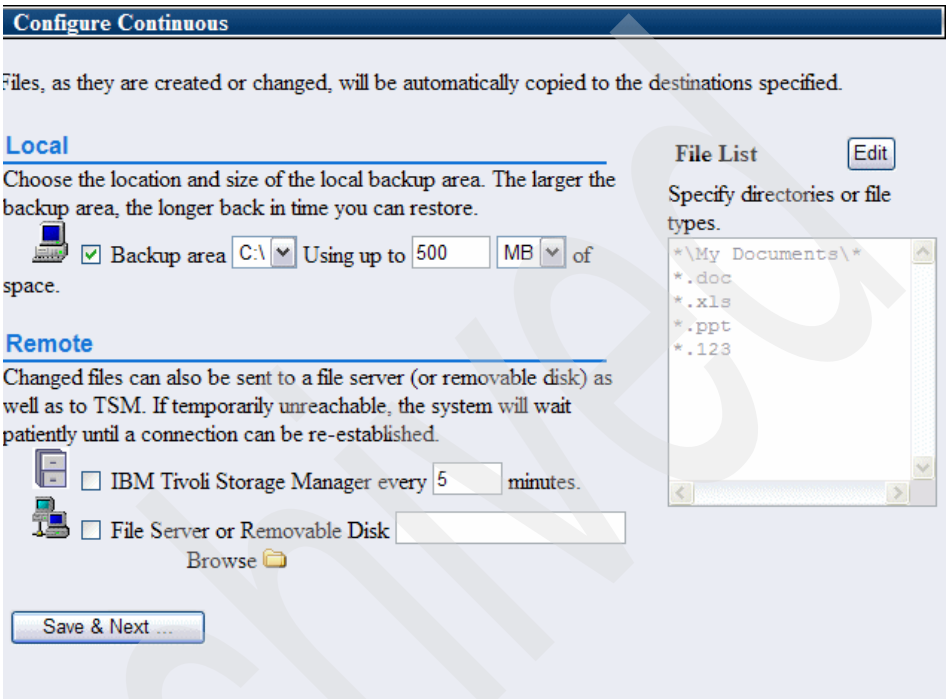


Figure 2-3 Configure continuous protection window

Initially, it has the following default settings:

- Local, Continuous backup to the local hard drive with the most available free space with a pool size of 500 MB.

  Although it is possible to uncheck the local replication option, we do not recommend doing this. However, you may want to select a different drive, based on your computer. For example, you may have the most free space on your C: drive, but you may prefer to have the backup files stored on another partition or drive. If you click the drop-down box, the list of known drives will show up for you to select.

You can also change the size of your backup pool. The default is 500 MB, which should be adequate for most users. One consideration for pool size is the size of the files you typically work with. If you make frequent changes to large files, you may want to increase the size of your pool. For example, if you have been working on a Word document and have backed up several versions, and then you edit a very large image file that is 300 MB, once you save the image file a second time, your pool will be purged of the older Word document versions.

- No remote backup.

  We highly recommend that you configure Tivoli Continuous Data Protection for Files for some sort of remote backup if you are connected, even intermittently, to some sort of external storage. If you commonly edit mission critical files several times during the day, continuous remote backup is the best way to make sure that you will be able to recover important files quickly in the case of hard drive failure. Otherwise, the Scheduled backup option is probably sufficient.

  If you have TSM client installed on your system, you can choose to have your changed files sent directly to your TSM server.[2] You can configure the TSM backup interval; use a shorter time, 5 minutes, if you change and save files in short time increments, or a longer time, 30 - 60 minutes, if you save less often.

- File List with \My Documents\ and common file extensions.

  If you save documents someplace other than the \My Documents\ path, it is important to make sure they get added into your File List so they will be included in the continuous backup. You can either specify this by directory path or file extension. For the directory path, you do not need to include the entire path. You just need to include enough to uniquely identify where your files are stored. For example, if you have saved files in:

  C:\work docs\critical\ and C:\work docs\misc

  You can add \work docs\ to the file list to include all of these files, or you can add \critical\ if you do not want to include the files in the \misc\ directory. Basically, Tivoli Continuous Data Protection for Files will search through your directory structure until it comes up with a match for your directory string, and will protect all files under that directory tree.

  You can also add file extensions, which will match the extension regardless of what directory it is saved in. This is useful for cases where you save certain types of files in a number of different directories. You can also use the directory and file extension in combination. For example, if you want to

[2] In the next release of Tivoli Continuous Data Protection for Files Version 2.2, releasing in June 2006, it will no longer be necessary to have the TSM client installed on your system.

include .jpg files in your \trip pics\ folder, but not other types of files in that directory, you could include \trip pics*.jpg.

Important: If you use the navigation links on the left panel of the GUI to change which window you are on, any changes you made on that window will not be saved. Make sure you use the **Save & Next** button whenever you make any changes to a configuration window.

After you are done reviewing and editing this window, click the **Save & Next** button at the bottom of the pane. You will then see the Scheduled protection configuration window.

Scheduled protection

By default, the Scheduled protection is disabled. If you choose to enable Scheduled protection, the default file list is everything on your computer that is not in your Exclude list. See “Exclusions” on page 35 for a description of this list.

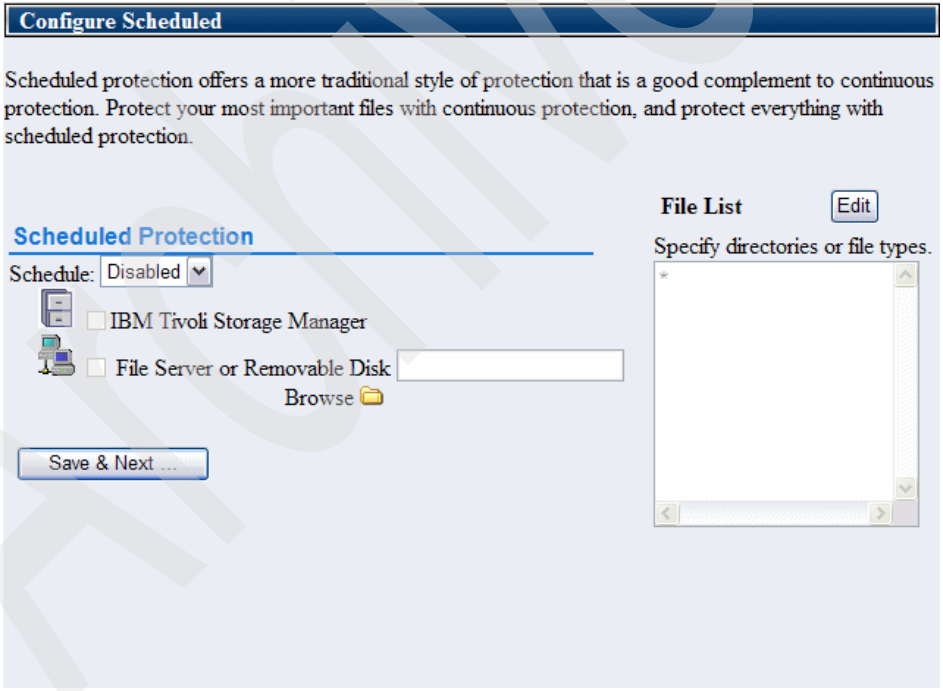


Figure 2-4 Configure scheduled protection window

You can choose to enable scheduled backup to either an existing TSM server, or to some external storage. (You could do both, but that would probably be unnecessary.) For TSM, you must already have the TSM client installed and running on your system. See the section on 2.2.2, “Do I need scheduled backup?” on page 27 to determine whether you want to enable scheduled protection.

You will need to select a backup interval. Even though you can configure the scheduled protection for as often as once per hour, we recommend that you select a longer interval. In general, a weekly backup is probably sufficient, unless your system is likely to change a lot during the course of a week. The hourly backups occur at the top of the hour, daily backups begin at midnight, weekly backups start just after midnight on Sunday morning, and the monthly backups start just after midnight on the first of each month.

Note: The actual start time of the backups is six seconds after the time interval. This can be configured in a larger environment to stagger the backup times to a single server. To change the time, open a command prompt window and navigate to the Tivoli Continuous Data Protection for Files installation directory. Then type:

```
fpa config-set targetbackupTime="#"
```

where # represents the number of seconds after the time interval you would like the backup to begin.

For the remote storage location, if you have already selected a share for continuous remote backups, that will also be used as your scheduled backup location. Tivoli Continuous Data Protection for Files will back up one copy of all of your files, so there needs to be enough space on the remote target to accommodate the approximate size you currently use on your hard drive. (This will be somewhat less given the exclusion list.) The default pool size for versions of your files is 5 GB. This is on top of the storage consumed by the initial backup. If you do not want to store versions of your files, you can set the pool size to 0, and then you will only back up the latest versions of your files. Tivoli Continuous Data Protection for Files will never remove files from the “latest version” set, it will only cycle versions out of the pool, with the oldest deleted first.

See 2.3.3, “Advanced configuration” on page 38 for a description of more configuration options for scheduled protection, including setting the number of versions.

After you are done reviewing and editing the Scheduled protection configuration window, click the **Save & Next** button. You will see the Exclusions window.

Exclusions

The default exclusion list is designed to cover the primary, known directories and file types that are not recommended for backup using this product. The list is shown below in Figure 2-5. This list has been developed over time, and we do not recommend removing any items unless you have a compelling reason to do so.

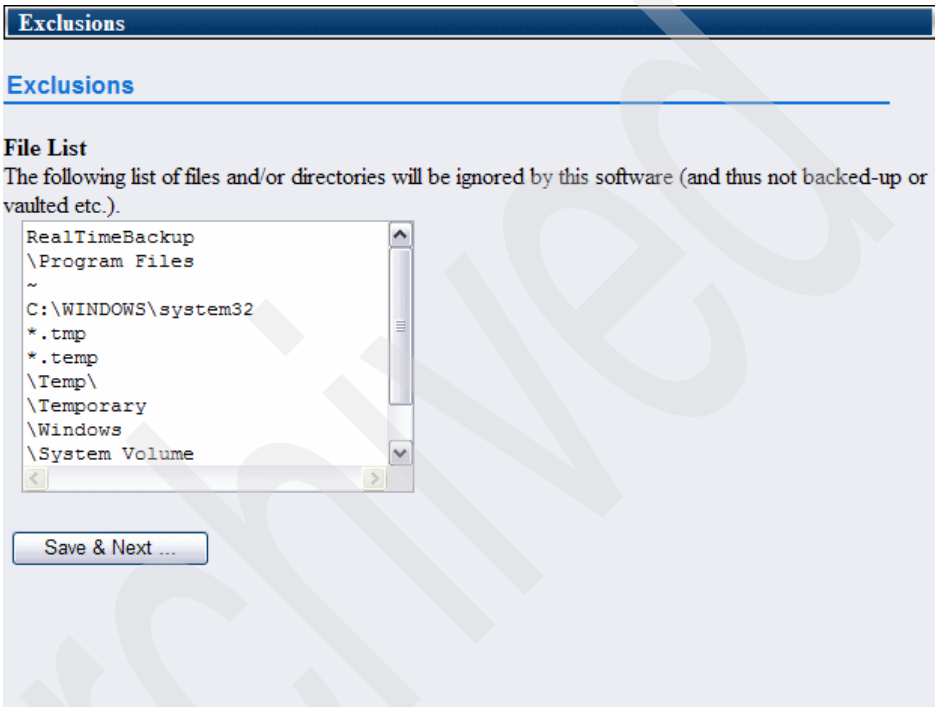


Figure 2-5 Configure exclusions window

To add an item to the exclusion list, click in the box at the end of the current list, and type your item on a new line.

Note: Keep in mind that the exclusion list gets processed *before* the inclusion lists for continuous, scheduled, and vault protection. So, anything in this list will never get backed up, even if the directory path or file extension falls under your inclusion lists.

If you happen to know of some type of file or directory that you do not want to have backed up, you can add it at this time. You can also come back to this window later and add items as you learn how Tivoli Continuous Data Protection for Files is working on your computer. See “Fine tuning” on page 41 for more information on how to decide what to add to your exclusion list.

When you are done reviewing and editing the exclusion list, click the **Save & Next** button. You will see the Synchronize window (Figure 2-6 on page 37).

Synchronize

The most important consideration for the Synchronize window is deciding when to synchronize, if at all. You do not have to synchronize your source and target locations if you simply want to start backing up file changes which occur from this point in time onwards. If you do want to synchronize, or pre-seed the backup locations with current versions of all of your files, there are several points in time where you may want to do this:

- At installation time

  If you are satisfied with the configuration you have and do not intend to change the configuration in the near future, now is a good time to synchronize. You can always re-synchronize later if you change your configuration.

- After you have tuned your settings to be most efficient for your needs

  See “Fine tuning” on page 41 for more information on tuning.

- After you have changed your configuration, especially your inclusion list

  For example, if you install new software and you realize that the files you save using that software are not being backed up, you should add either the directory path or the file extension to your file inclusion list. We recommend that you re-synchronize at this time.

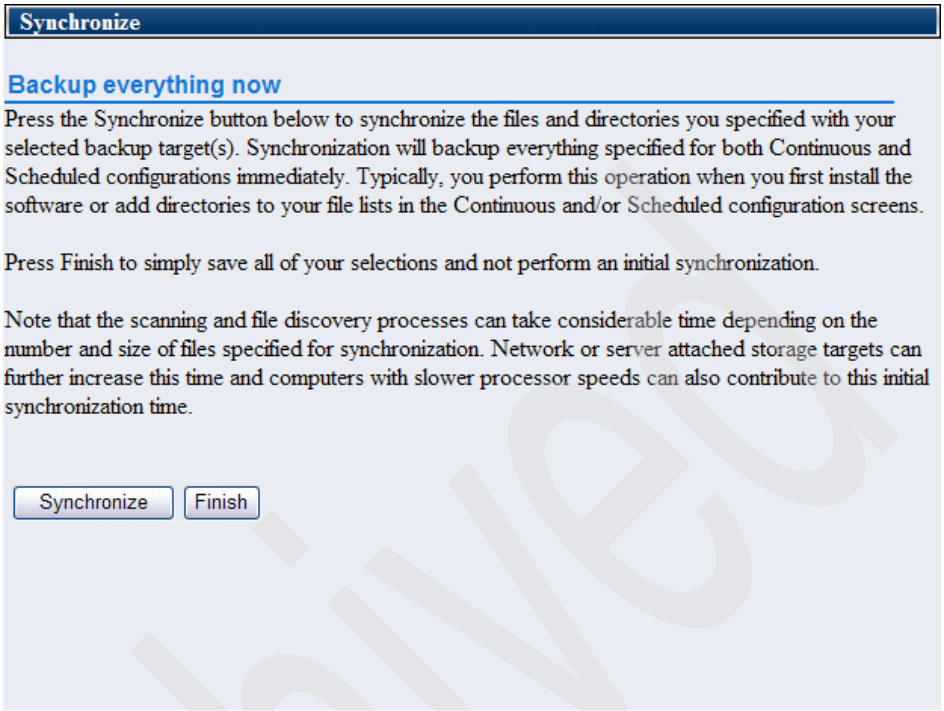


Figure 2-6 Synchronize window

Note: Your initial synchronization could take several hours, and it may significantly reduce the amount of system resources you have to work using other software. So, we recommend that you plan your initial synchronization accordingly.

If you decide to synchronize at this time, click the **Synchronize** button. You can monitor the progress of the synchronization by clicking the link to the Activity window under the Advanced section. See 2.4.3, “Activity” on page 48 for more information on what you will see on this window.

If you choose not to synchronize, or when synchronization is complete, click the **Finish** button to save all changes. You will see the Activity window, which displays all current activity. You can close the GUI at this time. Even when you close the GUI, Tivoli Continuous Data Protection for Files is running in the background and protecting your files.

2.3.3 Advanced configuration

There are several options that you might wish to set up either at the time of initial configuration, or after you have been using the product for a while.

Vault

When you select directories or file types for the Vault function, this means that those files cannot be altered in any way, either edited or deleted. The Vault function allows you the option of either setting up a directory path for your vault, or selecting a file extension for inclusion. The Vault file list works in the same manner as the other inclusion lists, so you can click in the white text entry box and type each entry on a separate line. You do not have to have a special Vault directory set up before you complete the configuration. Tivoli Continuous Data Protection for Files will start protecting files whenever you create the directory and start putting files in it.

Note: The exclusion list is in effect for the Vault activity as well, so you need to make sure that your intended Vault files are not on your exclusion list.

Make sure you click the **Save** button after making any changes to the file list.

Figure 2-7 on page 39 shows the Vault window.

Figure 2-7 Vault window

The Vault feature can also be used to keep your documents safe from editing and deletion for a specified period of time. In order to use this function, you need to create a directory called \Keepsafe under one of your Vaulted directories. For example, you could add \SecureDocs\ to your Vault File List and then create the following directories, \SecureDocs\Keepsafe\ to your hard drive. Once you have done this, all files under the \SecureDocs\ directory path will be locked so that they can never be edited or deleted. In addition, you can then add directories under the \Keepsafe\ directory path if you have files that can be deleted or edited after a certain point in time.

The Keepsafe directories follow a naming convention that indicates how long you want to keep your files safe. For example, you could have:

- \Retain 3 years\
- \Retain 60 days\
- \Retainuntil 2010-06-30

Any files placed in one of these directories will be kept unaltered for the specified amount of time. After the retention period is up, these files can be deleted. This can be useful in cases where you want to purge your hard drive once the critical retention time us over. See *Tivoli Continuous Data Protection for Files Version 2.1. Installation and User's Guide*, GC32-1783 for more information on the exact syntax of these directories.

Advanced settings

The Advanced Settings window (Figure 2-8 on page 41) allows you to adjust the configuration parameters for your remote target, as well as for the replication engines. For most users, the default settings on this window should give you the performance you need.

Important: Changing the settings on this window can have a significant impact on your machine performance and the behavior of Tivoli Continuous Data Protection for Files. Please make sure you fully understand the ramifications of the changes you are making before committing the changes.

The default configuration for remote targets is shown in Figure 2-8 on page 41 on the top half of the window. You might want to change the values here for several reasons:

- If you have limited storage space on your remote file server, you can decrease the size of the space allocated for the remote.
- If you are not backing up very large files very often, you may want to increase the size limit on the files that are excluded from versioning.

It is important to remember that these settings affect both the continuous and the scheduled remote replication activity.

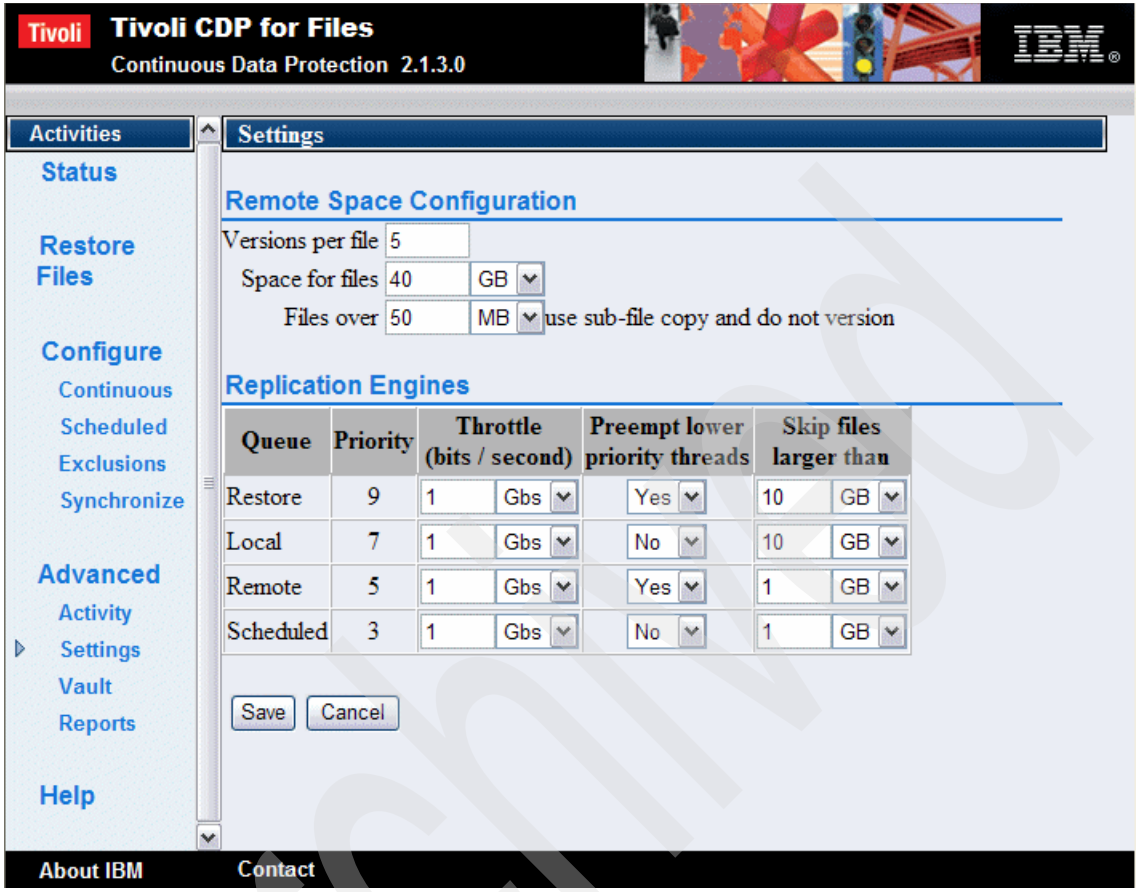


Figure 2-8 Advanced settings window

Fine tuning

We recommend that you take a little time to check your configuration after you have been up and running for a few days, and again periodically, to make sure that Tivoli Continuous Data Protection for Files is running efficiently and including all of your most important files.

There are basically two questions you need to answer while fine tuning:

1. Are my critical files getting backed up where I need them?
2. Are there extra files I do not need getting backed up that are taking up storage space?

The easiest way to check this is to look directly in your \RealTimeBackup folder on your hard drive. You can navigate there directly in a Windows® Explorer window and look down into the subdirectories to see what is getting backed up. At the first level, under the \RealTimebackup folder, you will see the drive letter you have selected to have backed up. Under this will be the actual backup directory structure that mirrors your hard drive directory structure. That is, for every directory on your hard drive that has files that have been backed up, that directory will be in your \RealTimeBackup directory structure. You will not see other the other directories from your hard drive, for example, the excluded directories like \Program Files and \Windows.

Note: Your \My Documents\ folder is usually found under C:\Documents and Settings\{username}\My Documents.

As you look through the directories, you will see all of the files that are being backed up. Think about the files you have been working on and other important files you have. Are these files present in your \RealTimeBackup directory structure? If you are missing some files, you may need to add them to your File Lists for inclusion, or check your Exclusion list to make sure they are not being excluded.

Also, if you see directories and files that you do not want backed up, you can note which directories are not needed and add them to your exclusion list. Only do this if you are sure that you will not need to restore files from these directories. The benefit of adding them to the exclusion list is that you will conserve space in your pool to make sure that you have the maximum room available for your most important files. You can also manually delete these directory trees from your \RealTimeBackup directory structure.

To do a more complex analysis of your backup configuration, you can also do a search using the Windows search tool by selecting **Start** → **Search** → **For Files or Folders**. When the tool appears, select your hard drive to search and have it search by modification date, for example, under “When was it modified,” select “Within the last week.” Also, under the “More advanced options” section, check off “Search system folders” and “Search hidden files and folders.” This will most likely produce a lengthy list of files, only some of which are files you have saved yourself during the week. Review the list of files that have changed in your normal directory structure, and verify that these same files are listed under the \RealTimeBackup folder directory in the same list. This may take a little time to check each file, but it is a good way to identify files that are being missed during the backup process.

Again, if there are files that are being missed, or extra files getting backed up that you do not want to include, you can edit your inclusion and exclusion file lists.

Note: You only need to perform this fine tuning on your local backup location. However, you can also manually clean up your network location if you found a large number of files getting backed up that you do not want.

2.4 Using Tivoli Continuous Data Protection for Files

Once you have the product installed and configured, you can generally forget about it and let it run in the background, knowing that your important files are being protected. However, there are a few situations where you will need to open the Tivoli Continuous Data Protection for Files GUI. The most critical function you will use after the initial configuration is restoring a file or files. The other functions involve monitoring your backup activity, adjusting your configuration, and other administrative activities. To open the Tivoli Continuous Data Protection for Files GUI, you can either select **Start** → **Programs** → **Tivoli** → **CDP for Files** → **IBM Tivoli Continuous Data Protection for Files**, or double-click the icon in your systray.

2.4.1 Restoring files

You can use the Restore window (Figure 2-9 on page 44) when you have lost one or more files and you need to recover them. This could happen by accidentally deleting the file, copying over the file, or possibly as a result of a larger problem like hard drive failure. While Tivoli Continuous Data Protection for Files does not provide full system restore, it can be used to bring back your most important files.

Open the Tivoli Continuous Data Protection for Files GUI and click the **Restore Files** link in the Activities window. The default location to back up from is your local backup, since this is the most common situation. You can change to another backup location, for example, your remote location, if the files you need are not on your local drive.

Note: If you want to restore files from your TSM Server, you will have to use the TSM client interface to access those files.

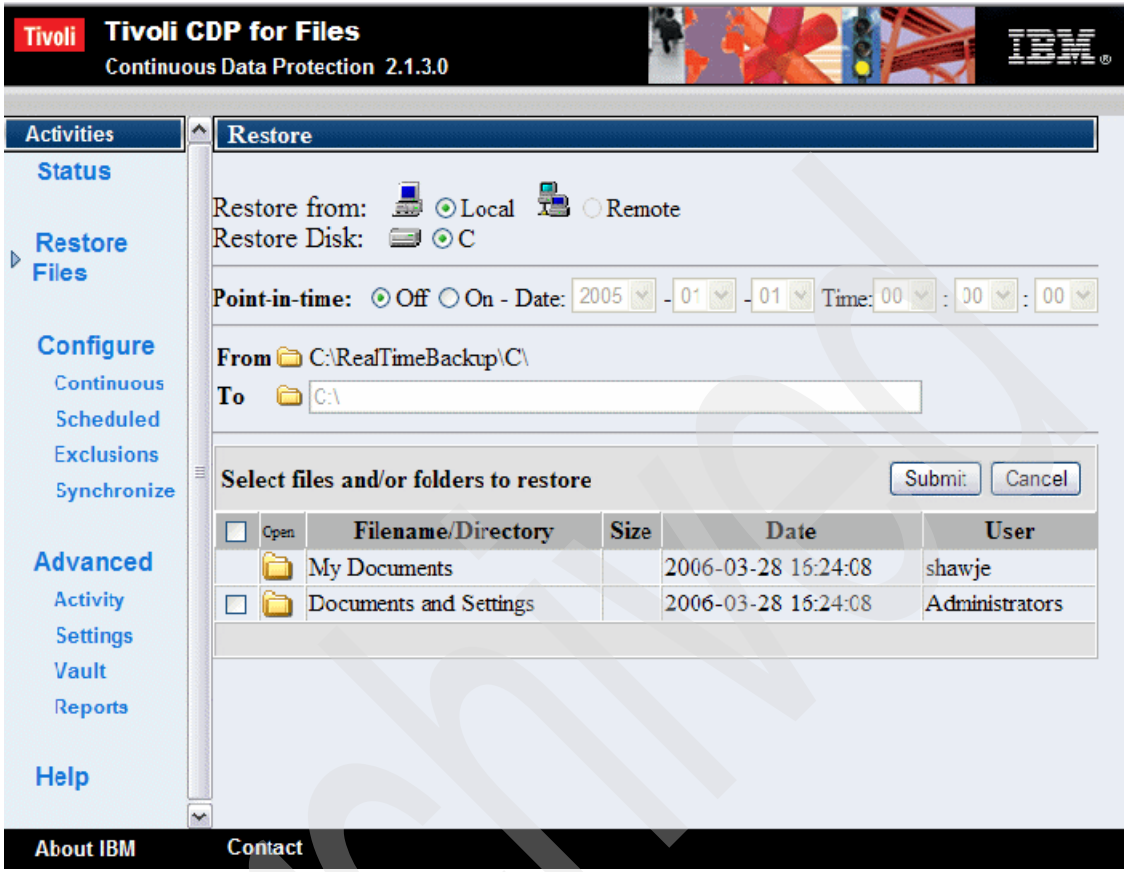


Figure 2-9 Restore window

To restore a single file or directory, simply navigate through the directory structure by clicking the folder icons to drill down through your directories. Once you have found the file or directory, select the check box in the left column and click the **Submit** button. This will take the latest version of each file and restore it to the location it came from. This will overwrite any existing files and change the name to the original name, if the file had been versioned.

If you need to restore a particular version of a single file, you can click the icon in the Open column next to the individual file. This will display all versions of the file, along with the time and date stamp from when it was backed up. You can then select the version you want to restore.

There are several options on this window that give you more flexibility and control over the restore activity. First, if you need to restore files, but do not want them to overwrite your current files, you can change where the files get restored to. Simply click the folder icon next to the **To** location, which lists the source directory by default. You can then browse to a new location to restore the files. This can be particularly useful in the case where you are doing a Point-in-Time restore. If you turn on the Point-in-Time restore option, you can restore all files (or a single file) back to the version that existed at a particular point in time. If you are restoring a large directory structure, but you have one or more files in the original directory tree that you do not want to overwrite (for example, you have edited and saved them recently), you can select to restore to a different top level directory and preserve the files you need. Then you can use the standard Windows Explorer window to move or copy the files where you need.

You can also choose to copy your files from the backup directory manually using the Windows Explorer or command-line functions, but then your versioned files will have the Tivoli Continuous Data Protection for Files time stamp code appended to the file name. You can rename the files once you have copied them, or open and do a Save As to return them to the original file name.

2.4.2 Status

The Status window (Figure 2-10) is a useful tool for monitoring your backup activity. The information includes a list of the most recent transactions, the number of files that have been backed up and which are pending, and how much space is being used on the local and remote backup locations.

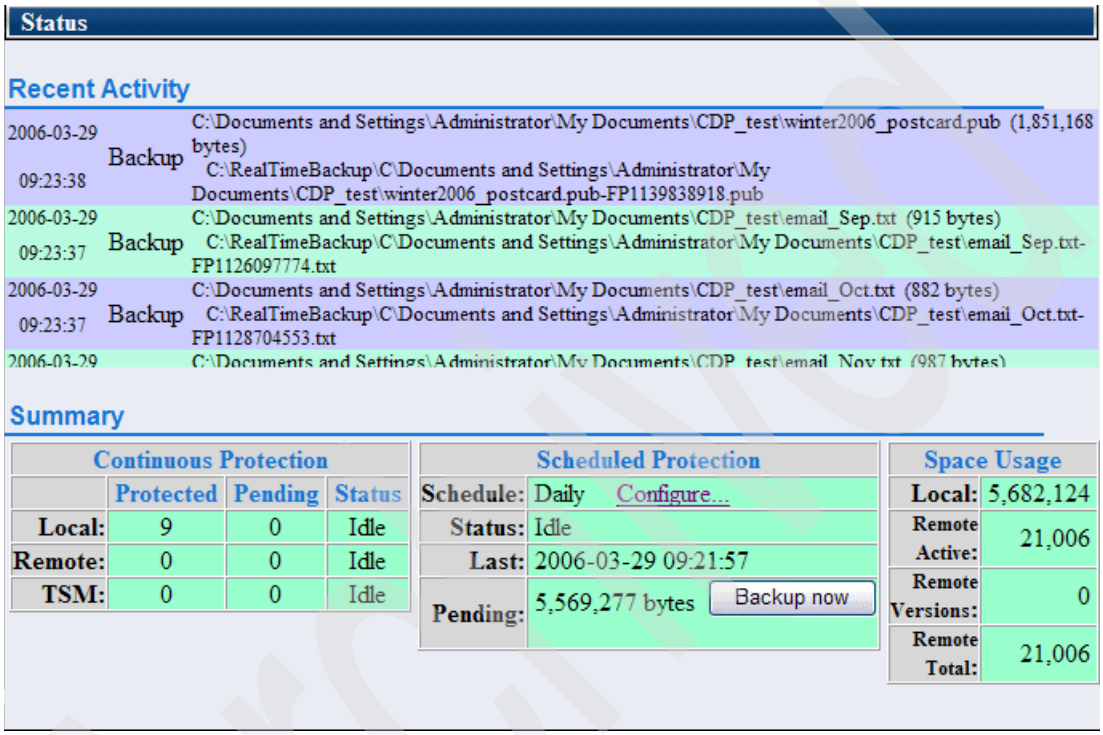


Figure 2-10 Status window

The Recent Activity portion of the window is useful for verifying that your backups are completing successfully. A normal backup will display “Backup” in the row with the date, time stamp, and source and target locations of the file that has been backed up. You will also see Version, Mkdir, Rename, Unlink, and Report in this column, all of which indicate successful activity in creating versions and directories on the remote target, deleting directories on the target, and posting information to the reports on the remote server. If Tivoli Continuous Data Protection for Files encounters a problem with the activity that it cannot resolve, you may see Badfile in this column.

The Continuous Protection table indicates how many files have been protected since the last boot up of the computer. The pending column reports how many actions are waiting to be processed on the target locations.

Note: The number in the pending column does not represent only the number of files to be backed up. It includes all activities, versioning, creating, or renaming directories, and so on, so this number will be higher than the actual number of files that will be copied.

The Scheduled Protection table displays your current schedule configuration, the date and time of your last backup, and the amount of content that is waiting for your next scheduled backup. It is a good idea to check this if you know that you are going to be disconnected from your remote backup target during the scheduled backup time. It may not be crucial if your configuration is set for Daily backups, or if you are configured for continuous remote backups, but if you are on a weekly or monthly schedule, you might want to click the **Backup now** button to make sure that your remote target is synchronized before you separate from your network target.

The Space Usage section can be a useful tool for checking to see how quickly you are filling up your pools, both Local and Remote. If the space is filling up and you have not been using the product for a very long time, say only a few weeks, you might want to consider enlarging the size of your pool. Alternatively, you might want to take a look at what files are getting backed up and adjust your Include and Exclude lists to further limit what is getting replicated. See “Fine tuning” on page 41 for more information on how to prune your pools and refine your lists.

2.4.3 Activity

The Current Activity window (Figure 2-11) displays a live view of what Tivoli Continuous Data Protection for Files is doing behind the scenes. It can be useful to view this activity at different times. For example, when you choose to Synchronize your source and target locations (either initially, or after some changes have been made), you may want to monitor the progress of this initial backup. It can also be useful to visit this window if it appears that Tivoli Continuous Data Protection for Files is taking an unusually long time to perform an activity, or if your system resources seem to be limited.

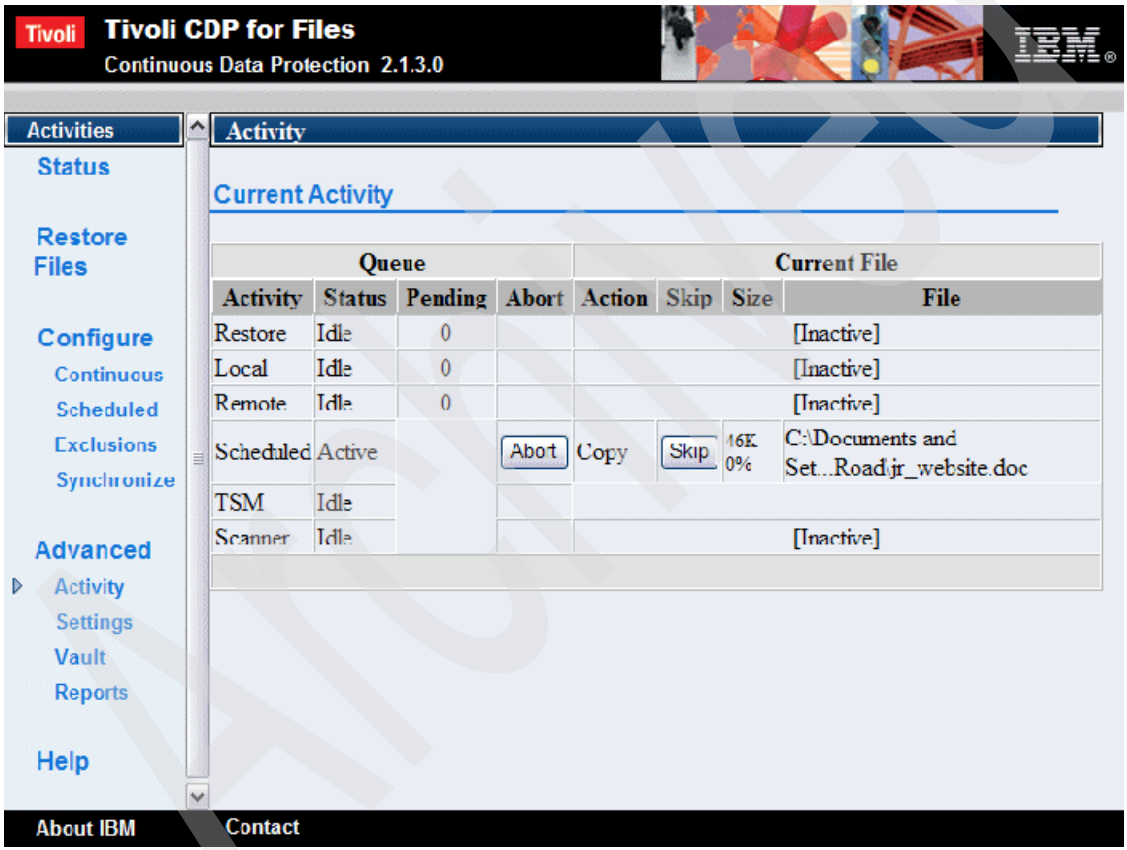


Figure 2-11 Current Activity window

When Tivoli Continuous Data Protection for Files is actively backing up files, you will see that activity happen on this window. You can use this window to have some idea of what files are being backed up and which processes are active. You can also choose to skip backing up an individual file or abort the backup entirely.

It is possible that you could have files included for backup that are very large, yet you do not really need them backed up, or at least not at the current time. You can click the **Skip** button.

It is also possible that you may have started a Synchronize or scheduled backup and it is taking up more of your system resources than you want at this point in time. You can use the **Abort** button to cancel the backup activity and then restart the activity later when it is a more convenient time.

2.4.4 Reports

The Reports window (Figure 2-12) provides an interface for easily finding and viewing information related to the remote backup activities. It also allows administrators in a large deployment of Tivoli Continuous Data Protection for Files to set up a single configuration and push it to end users from a central location.

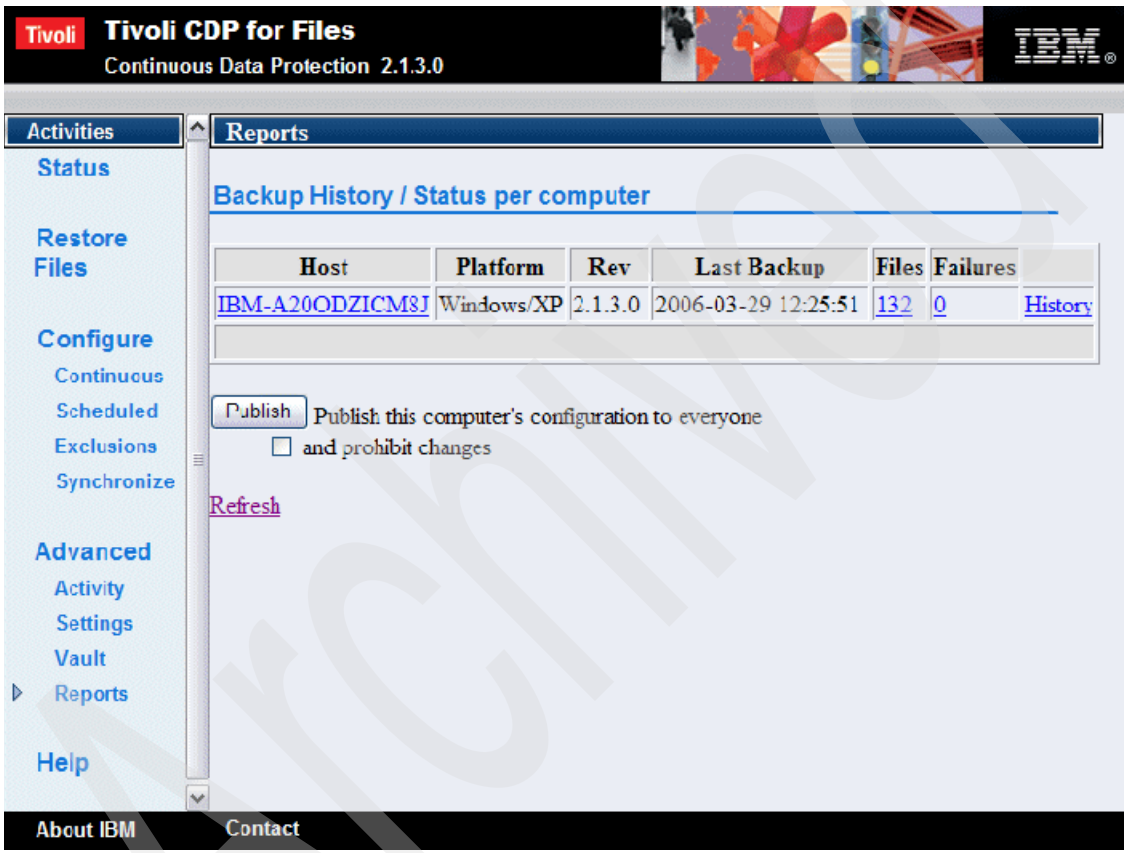


Figure 2-12 Reports window

If you have multiple computers backing up to the same location, you can view reports from each computer. The Host column displays current configuration information, the Files column displays the files backed up in the latest backup, the Failures column displays a list of files that failed to replicate (if any), and the History link brings you to a page with a list of previous logs, including error logs.

3

Troubleshooting, hints, and tips

In this chapter, we discuss some troubleshooting methods, hints, and tips for running the Tivoli Continuous Data Protection for Files. It covers potential installation issues, and replication problems, as well as operational issues in conjunction with the IBM Tivoli Storage Manager (TSM). We also provide some information about the log files used by the Tivoli Continuous Data Protection for Files and show how to trace the program.

Note: While installing, configuring, and operating the Tivoli Continuous Data Protection for Files, you may experience various kinds of problems. In this chapter, we cover some problems that are common. However, it is not possible to cover all potential problems. Therefore, if you face a problem that we have not described here, follow the normal support procedure to contact your local IBM support personnel. This chapter may help you to gather some information that you can hand over to the IBM support personnel for deeper problem analysis.

In particular, we cover the following topics:

- Installation issues
- Replication problems
- IBM Tivoli Storage Manager issues

- Log files and FPcommand.bat
- Tracing

3.1 Installation issues

This section contains information about some common problems that may arise during installation of the Tivoli Continuous Data Protection for Files, and how to solve and avoid these issues.

3.1.1 Disk space

By default, the Tivoli Continuous Data Protection for Files is installed in the directory C:\Program Files\Tivoli\CDP_for_Files. You can change the installation location to a different drive, path, or both, but this may lead to a problem if the new chosen location does not have enough free disk space to install the Tivoli Continuous Data Protection for Files.

Figure 3-1 shows an example of a non-default installation location, where the Tivoli Continuous Data Protection for Files is installed in the directory H:\Program Files\Tivoli\CDP_for_Files.

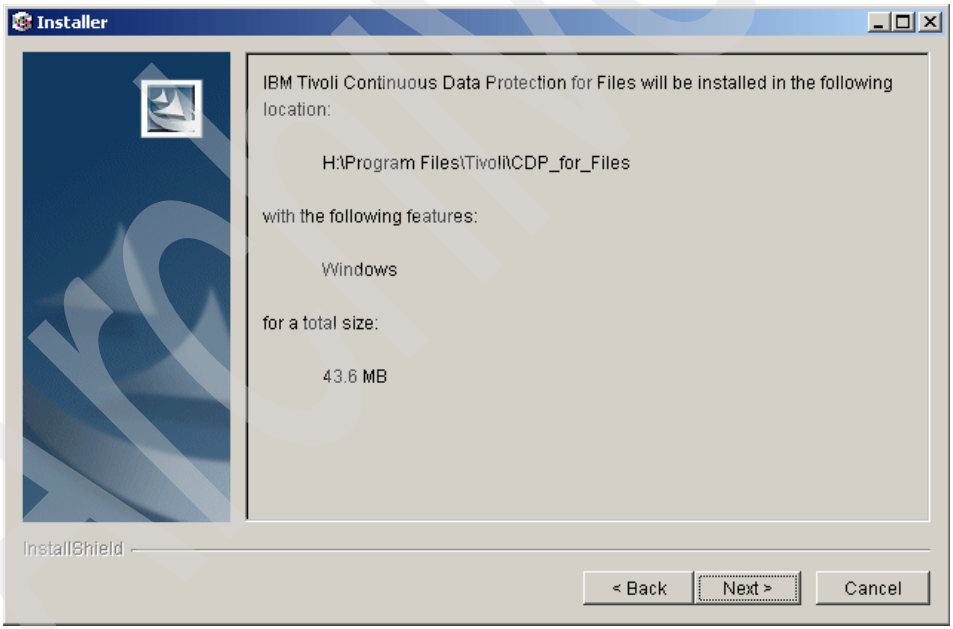


Figure 3-1 Installation summary window

As shown in Figure 3-1, the installation summary window shows that the complete installation of the Tivoli Continuous Data Protection for Files needs 43.6 MB of free disk space.

To avoid an incomplete and, therefore, unusable installation of the Tivoli Continuous Data Protection for Files due to insufficient disk space, precheck the disk space before beginning the actual installation. In case there is not enough free space available to hold a complete Tivoli Continuous Data Protection for Files installation, a warning window (see Figure 3-2) appears and the installation ends without installing anything when you click the **Finish** button.

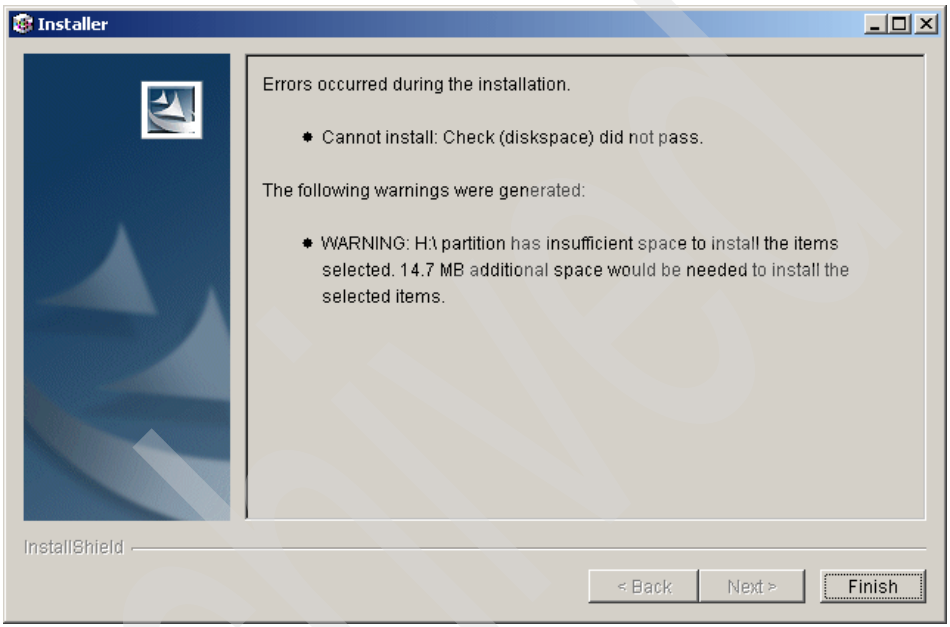


Figure 3-2 Insufficient disk space warning window

If you receive this type of installation warning, ensure that the installation location has sufficient free disk space available (in this case, at least 43.6 MB) for a complete and successful installation of the Tivoli Continuous Data Protection for Files.

3.1.2 Non-privileged users

The Tivoli Continuous Data Protection for Files works fine for all kind of users, even those users that have only limited privileges (non-privileged users).

Note: To configure the Tivoli Continuous Data Protection for Files in a multi-user environment, refer to 4.3, “Multiple users in a large enterprise environment” on page 126 and *Tivoli Continuous Data Protection for Files Version 2.1. Installation and User’s Guide*, GC32-1783.

However, to install the Tivoli Continuous Data Protection for Files on a system, the user needs to have *administrative rights*. This is necessary because besides the program files, the user needs to install low-level driver components as well as perform updates to the Windows registry.

To protect a system from unauthorized program installations, non-privileged users are usually not allowed to install programs into the program files directory. If a non-privileged user tries to install the Tivoli Continuous Data Protection for Files anyway, an error window is displayed informing the user that the destination directory is not writable (see Figure 3-3).

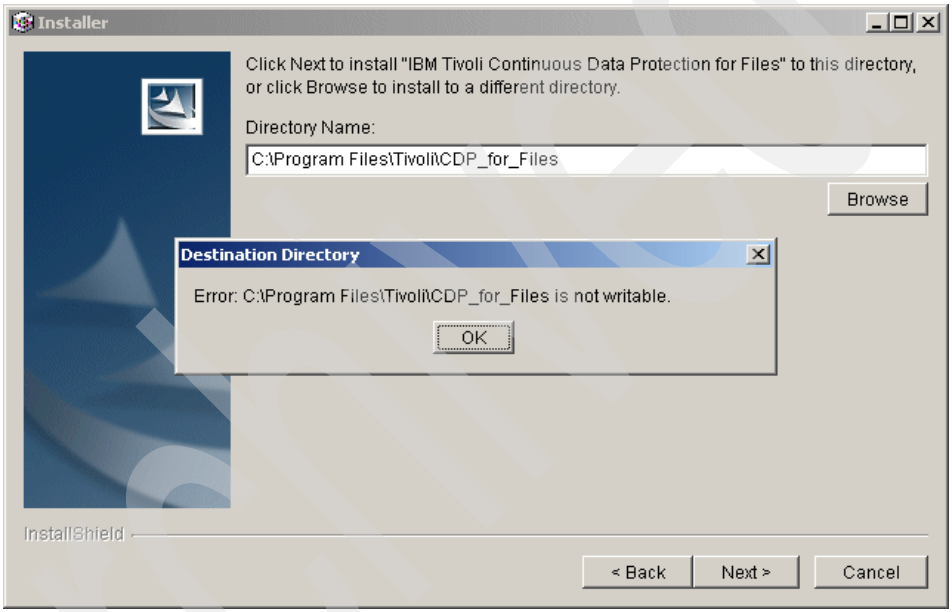


Figure 3-3 Error window due to write-protected installation director

Ensure that you have the necessary administrative rights to install the Tivoli Continuous Data Protection for Files or ask your system administrator to perform the program installation for you.

3.1.3 Port conflicts

To run the Tivoli Continuous Data Protection for Files and manage it via the Graphical User Interface (GUI), the Tivoli Continuous Data Protection for Files service is listening by default on port 9003.

Unfortunately, the user cannot change this port prior or during the installation process. In case another application is already using port 9003, the Tivoli Continuous Data Protection for Files service will later on fail to bind to it.

This section shows how the user can change the default port in the Windows registry after the installation is finished, and the Tivoli Continuous Data Protection for Files can operate again.

Important: If an application is already using port 9003, the installation of the Tivoli Continuous Data Protection for Files itself will not fail. All necessary files will be copied to the system and the required changes will be made in the Windows registry.

Checking for potential port conflicts before the installation

To display all the current connections and listening ports, use the **`netstat -a`** command. To do so, perform the following steps:

1. Click **Start** → **Run**, type **`cmd`**, and click **OK**.
2. In the command-line window that appears, enter the **`netstat -a`** command.

   Figure 3-4 shows the output of a **`netstat -a`** command *before* the installation of the Tivoli Continuous Data Protection for Files. A program is already listening on port 9003.

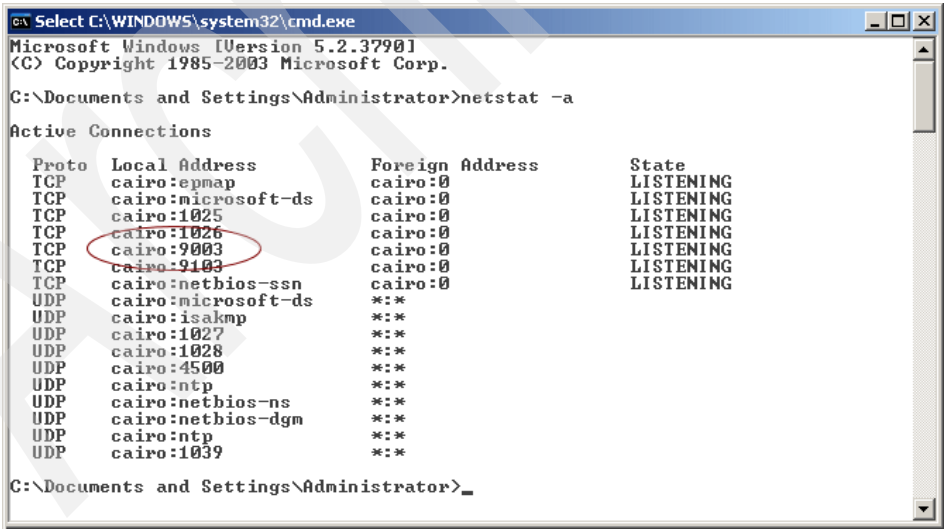


Figure 3-4 Another program already using port 9003

In this case, the Tivoli Continuous Data Protection for Files service will not be able to bind successfully to port 9003 after the installation is completed.

Installing the Tivoli Continuous Data Protection for Files

Refer to 2.3.1, “Installation” on page 29 for details about how to install the Tivoli Continuous Data Protection for Files.

At the end of the installation process

When the service tries to start for the first time at the end of the Tivoli Continuous Data Protection for Files installation process, a notification message informs you that the Tivoli Continuous Data Protection for Files is experiencing a problem (see Figure 3-5).

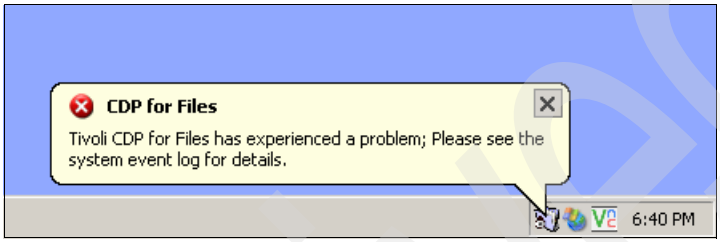


Figure 3-5 The Tivoli Continuous Data Protection for Files reporting a problem

Windows system event log

If you refer to the system event log in the Event Viewer, as requested by the Tivoli Continuous Data Protection for Files, the event log shows something similar to Figure 3-6 on page 58.

Depending on the Windows operating system that you use, follow these steps to start the Event Viewer:

- Windows XP:

  Select **Start** → **Control window** → **Administrative Tools** → **Event Viewer** → **System**.

- Windows 2000 and 2003:

  Select **Start** → **Settings** → **Control window** → **Administrative Tools** → **Event Viewer** → **System**.

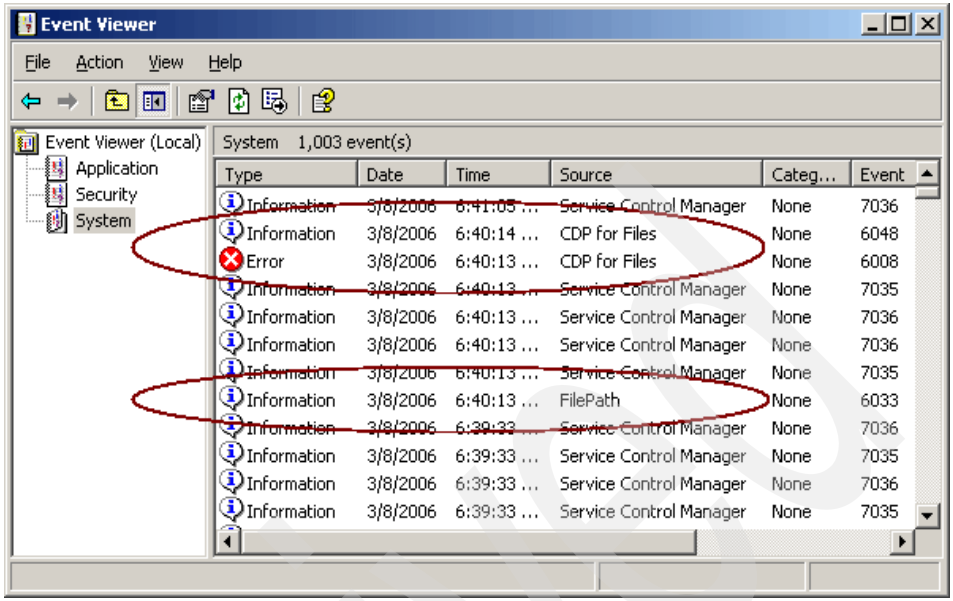


Figure 3-6 Tivoli Continuous Data Protection for Files entries in the event log

There are three log entries that belong to the Tivoli Continuous Data Protection for Files:

- Two informational log entries:
  - Source: FilePath

    Event ID: 6033

    Description: FilePath (host) driver loaded and ready
  - Source: CDP for Files

    Event ID: 6048

    Description: Tivoli CDP for Files daemon started successfully
- One error log entry:
  - Source: CDP for Files

    Event ID: 6008

    Description: During socket bind operation, failed; Reason: An attempt was made to access a socket in a way forbidden by its access permissions.

Figure 3-7 on page 59 shows the complete properties of the error event log entry due to the Tivoli Continuous Data Protection for Files not being able to bind to the port. You can get this window by right-clicking **Error log entry with Event ID 6008** and selecting **Properties**.

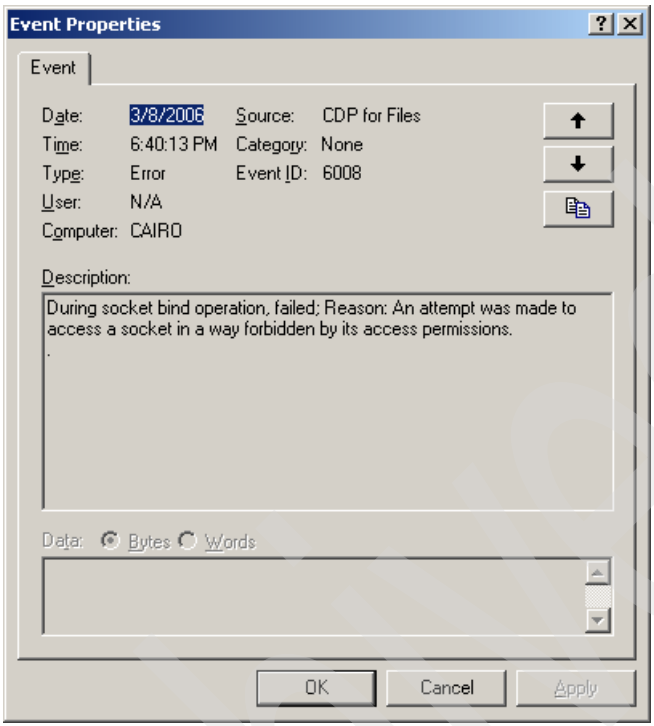


Figure 3-7 Error entry in the Windows system event log

Editing the Windows registry

To change the port number to a different unused port so that the Tivoli Continuous Data Protection for Files can work properly, edit the Windows registry using the Registry Editor.

We have explained the steps to make the changes in the Windows registry in detail, as an incorrect handling of the Registry Editor can seriously harm the Windows system's stability and ability to function.

Attention:

- If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. IBM cannot guarantee that you can solve the problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.
- We recommend that you make a backup of the Windows registry before making any manual changes to it. This allows you to restore the Windows registry in case something goes wrong accidentally.

Perform the following steps to make the necessary changes in the Windows registry:

1. To start the Registry Editor, select **Start** → **Run**, type **`regedit`**, and click **OK**.
2. In the left frame, locate and select the branch **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\FilePathsrv**

   Figure 3-8 shows that the port number (by default 9003) is stored in the DWORD Value named *FpPort*.

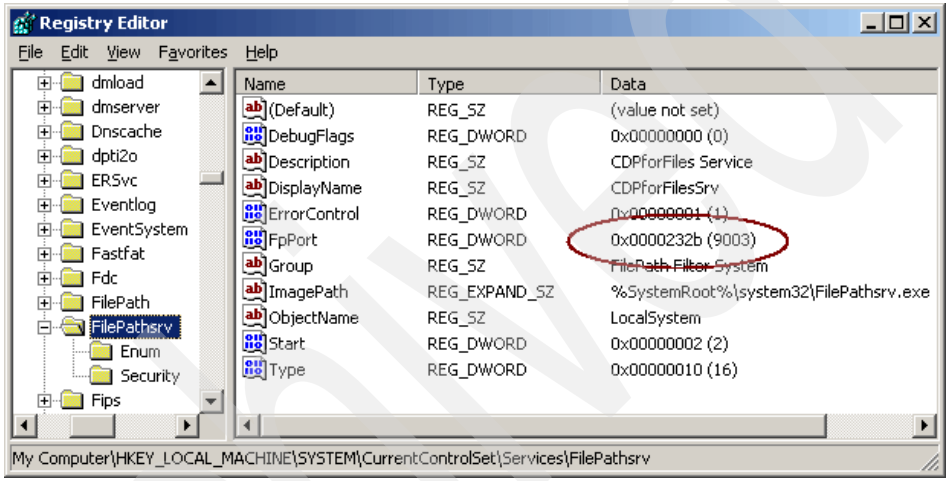


Figure 3-8 Port number in the FpPort DWORD Value

3. Right-click the **FpPort** DWORD Value, and select **Modify** (see Figure 3-9 on page 61).

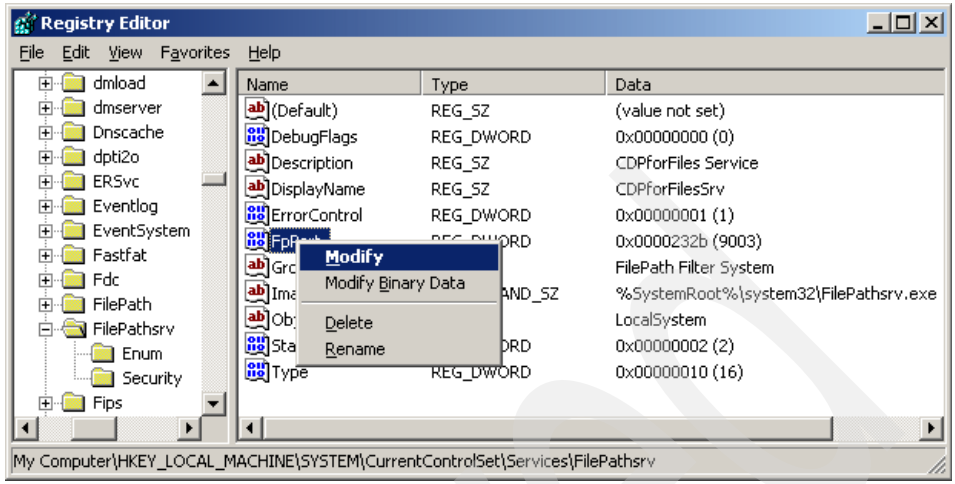


Figure 3-9 Modifying the FpPort DWORD Value

4. Select **Decimal**, enter an unused port number (for example, 9005) and click **OK** (see Figure 3-10).

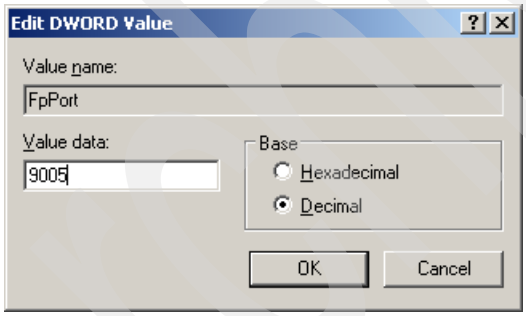


Figure 3-10 Changing the port number to 9005

Figure 3-11 shows the new port number (9005) in the FpPort DWORD Value.

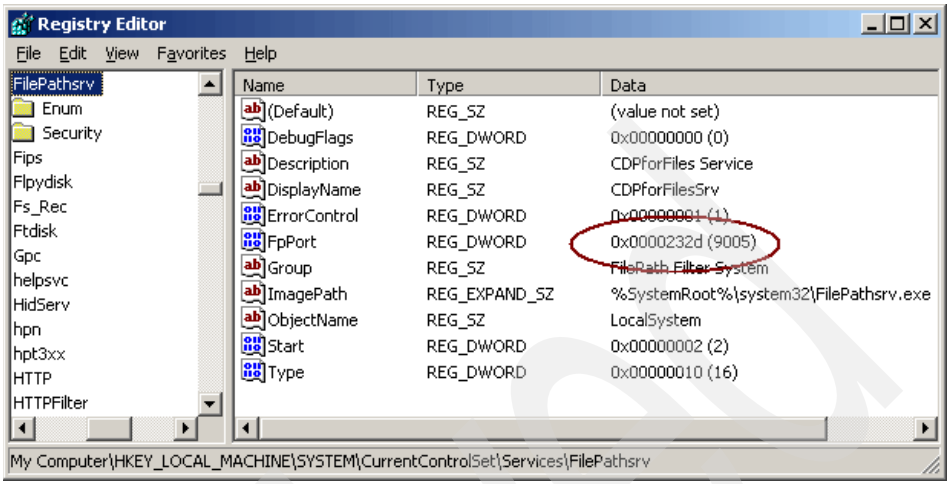


Figure 3-11 New port number in the FpPort DWORD Value

5. Click **File** and select **Exit** to close the Registry Editor. The changes you made are saved automatically.

Final steps

After changing the Windows registry, you have to perform two additional steps.

Modifying start.html

The Tivoli Continuous Data Protection for Files places a small icon in the notification area of the taskbar in order to notify you about incidents or informational messages (see Figure 3-5 on page 57). You can also use this icon to start the GUI of the Tivoli Continuous Data Protection for Files by double-clicking it.

When you double-click this icon, an Internet browser opens with the following file URL:

```
file:///C:/Program%20Files/Tivoli/CDP_for_Files/html/login/start.html
```

As shown in Figure 3-12 on page 63, the file start.html itself redirects to the URL `http://localhost:9003`, which includes the old port number.

Figure 3-12 The original start.html file with port 9003

You have to edit this file and change the port number of the URL to the same value that you entered in the Windows registry (in this case, 9005). To edit the start.html file, perform the following steps:

1. Select **Start** → **(All) Programs** → **Accessories** → **Windows Explorer**.
2. In the left frame of the Windows Explorer, locate and select the folder **C:\Program Files\Tivoli\CDP_for_Files\html\login**.
3. In the right frame, right-click the **start.html** file and select **Edit**. This starts the Notepad editor.
4. Change the port number from 9003 to 9005. The file start.html should now look like Figure 3-13.

Figure 3-13 The start.html file after editing (now using port 9005)

5. To save the changes, select **File** → **Save**.
6. Exit Notepad by selecting **File** → **Exit**.

Note: Usually, it is *not* necessary to make any manual changes to files like we did in this case with start.html. But if you have made any manual changes and you want to uninstall the Tivoli Continuous Data Protection for Files at some point in time, a message window will appear. This window informs you that the files have been modified, and asks if you want to remove the files. If you click **Yes** or **Yes to All**, the modified files will also be removed from your system.

Logging off / logging on and restarting the service

The last step to get the port conflict resolved depends on whether you are running the Tivoli Continuous Data Protection for Files as a logged-in application (which is the default) or whether you executed the FpForServers.js application so that the Tivoli Continuous Data Protection for Files runs as a real Windows service.

- Running as a logged-in application (default):

  If the Tivoli Continuous Data Protection for Files is running as a logged-in application, you have to log off and log on again.

- Running as a Windows service:

  In case the Tivoli Continuous Data Protection for Files is running as a Windows service, you have to restart the service by performing the following steps:

  a. Windows 2000 and 2003: Select **Start** → **Settings** → **Control window** → **Administrative Tools** → **Services**.

     Windows XP: Select **Start** → **Control window** → **Administrative Tools** → **Services**.

  b. Right-click the **CDPforFilesSrv** service and select **Restart**.

Note: For more information about FpForServers.js and how to use Tivoli Continuous Data Protection for Files on a file server, please refer to “Using Tivoli Continuous Data Protection for Files on servers” in *Tivoli Continuous Data Protection for Files Version 2.1. Installation and User’s Guide*, GC32-1783.

Checking the proper functioning

Finally, you need to check if everything is working as expected and that the Tivoli Continuous Data Protection for Files is using the new port.

Using the netstat -a command

To check whether the new port (9005) is listened to, use the **`netstat -a`** command again. Figure 3-14 on page 65 shows the output of a **`netstat -a`** command *after* you have changed the port number.

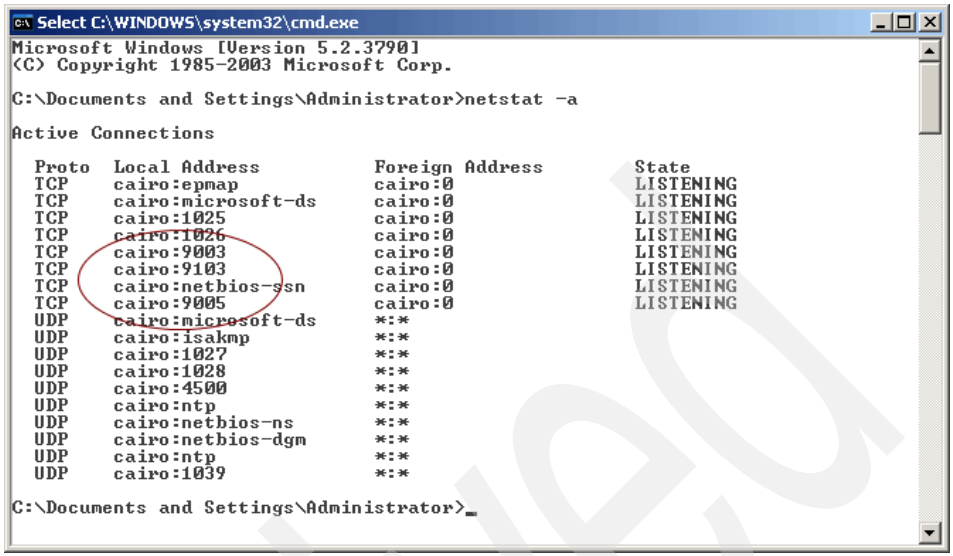


Figure 3-14 Netstat -a output showing the usage of the new port 9005

In the Event Viewer, you can also see that the Tivoli Continuous Data Protection for Files is able to listen on port 9005 (see Figure 3-15).

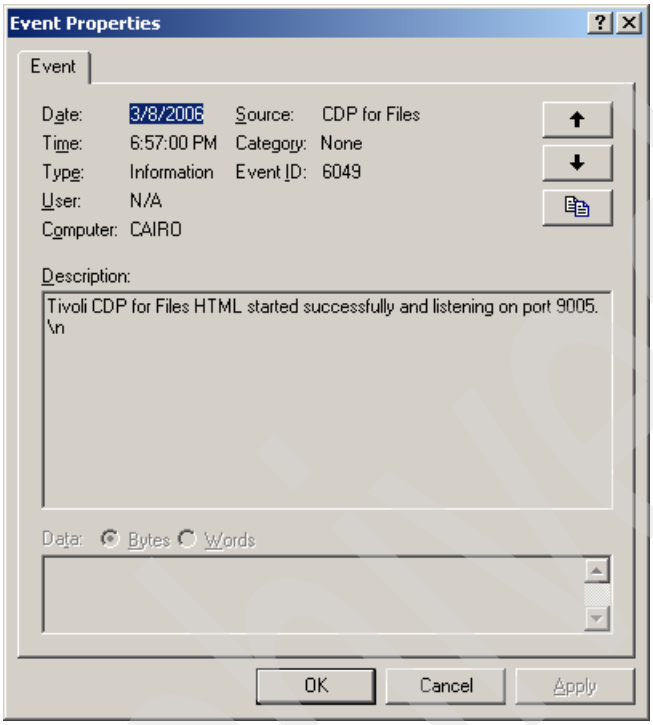


Figure 3-15 Successful entry in the Windows system event log

Figure 3-16 on page 67 shows the administrative GUI of the Tivoli Continuous Data Protection for Files using the new port 9005 (URL `http://localhost:9005`).

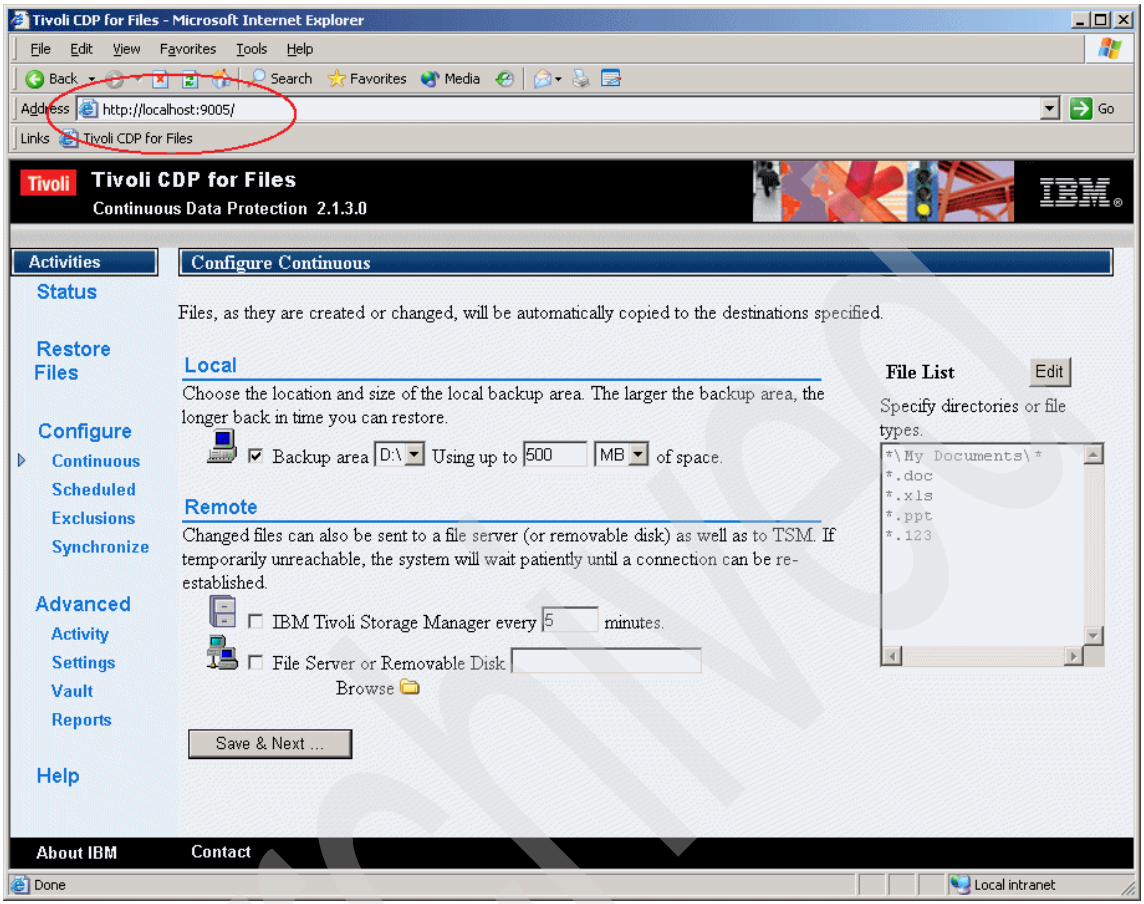


Figure 3-16 The Tivoli Continuous Data Protection for Files GUI using port 9005

3.2 Replication problems

This section covers some common (remote) replication issues. We will discuss potential problems you may experience if you are using a removable disk as a remote target for saving your files and in case you are storing files across the network on a file server for remote protection.

The following topics will be described in the section about using a removable (external USB-) disk as a remote backup target:

- Removable disk / file system is full
- Problem with changing drive letter assignments

When you store files on a remote file server, you may have to consider the following issues:

- Transient networks
- Universal Naming Convention[1] (UNC) names versus using drive letters

3.2.1 Removable disk issues

Using a removable (external USB) disk is a very common and convenient method for protecting data when there is no file server available as a remote backup target. For example, if you are travelling around with your mobile computer, you do not want to miss having an alternative backup location beside your local backup area in case your internal disk gets corrupted, so you can safely restore from the removable disk.

In the following example, we are using an external USB disk named “USB_Drive” with assigned drive letter (F:) as a remote backup location (see Figure 3-17 and Figure 3-18 on page 69).

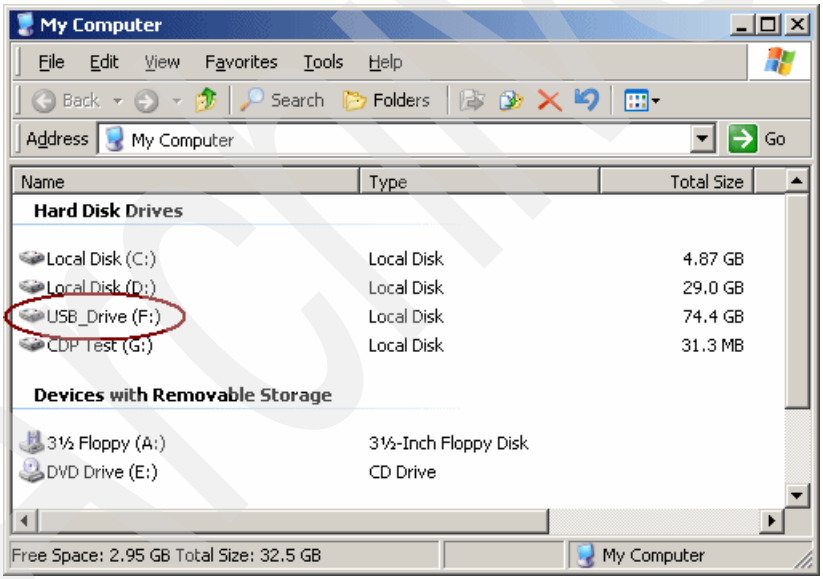


Figure 3-17 External USB disk named USB_Drive mapped as drive F:

[1] For information about Universal Naming Convention (UNC), for example, have a look at “Path (computing)”, found at:
http://en.wikipedia.org/wiki/Path_%28computing%29#Universal_Naming_Convention

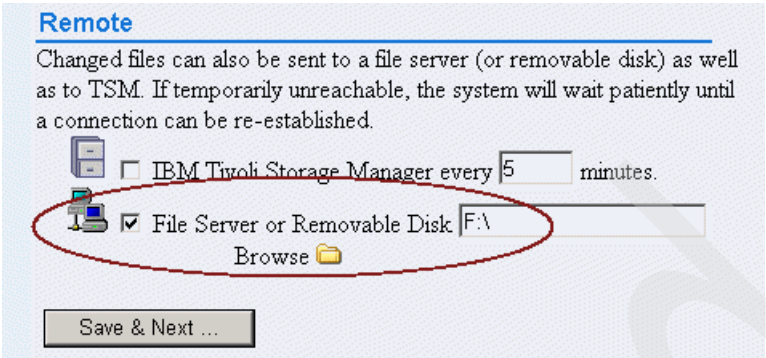


Figure 3-18 Drive F: (USB_Drive) as remote backup target

Disk / file system full

Due to the rising amount of data these days, an external USB drive may run out of disk/file space, though the sizes of removable disks have dramatically increased in the last couple of years. If Tivoli Continuous Data Protection for Files is facing a problem replicating to the specified remote location due to a disk / file system full condition, it lets you know about this by issuing the notification message seen in Figure 3-19.

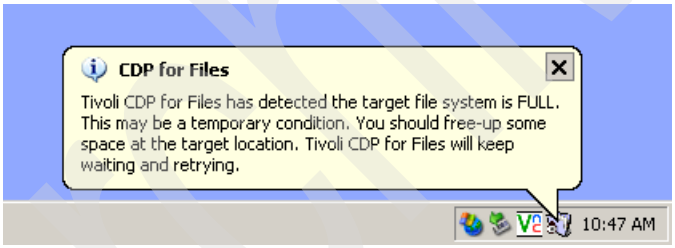


Figure 3-19 Disk full informational message

Important: Tivoli Continuous Data Protection for Files *will not* stop keeping track of the changes you make to your files even when you see this message. It will wait for some time and tries to replicate the changed files later again, as this may be only a temporary condition.

To avoid a disk / file system full condition, you can do either one or more of the following things:

- Free up some space on the removable disk or the remote file system.
- Open the Tivoli Continuous Data Protection for Files GUI by double-clicking on the Tivoli Continuous Data Protection for Files icon in the notification area, click **Settings** in the Advanced section area of the left frame, and adjust the Remote Space Configuration settings (see Figure 3-20):
  - Decrease the number of versions per file being stored remotely.

    or
  - Reduce the space being used for files on the remote location.

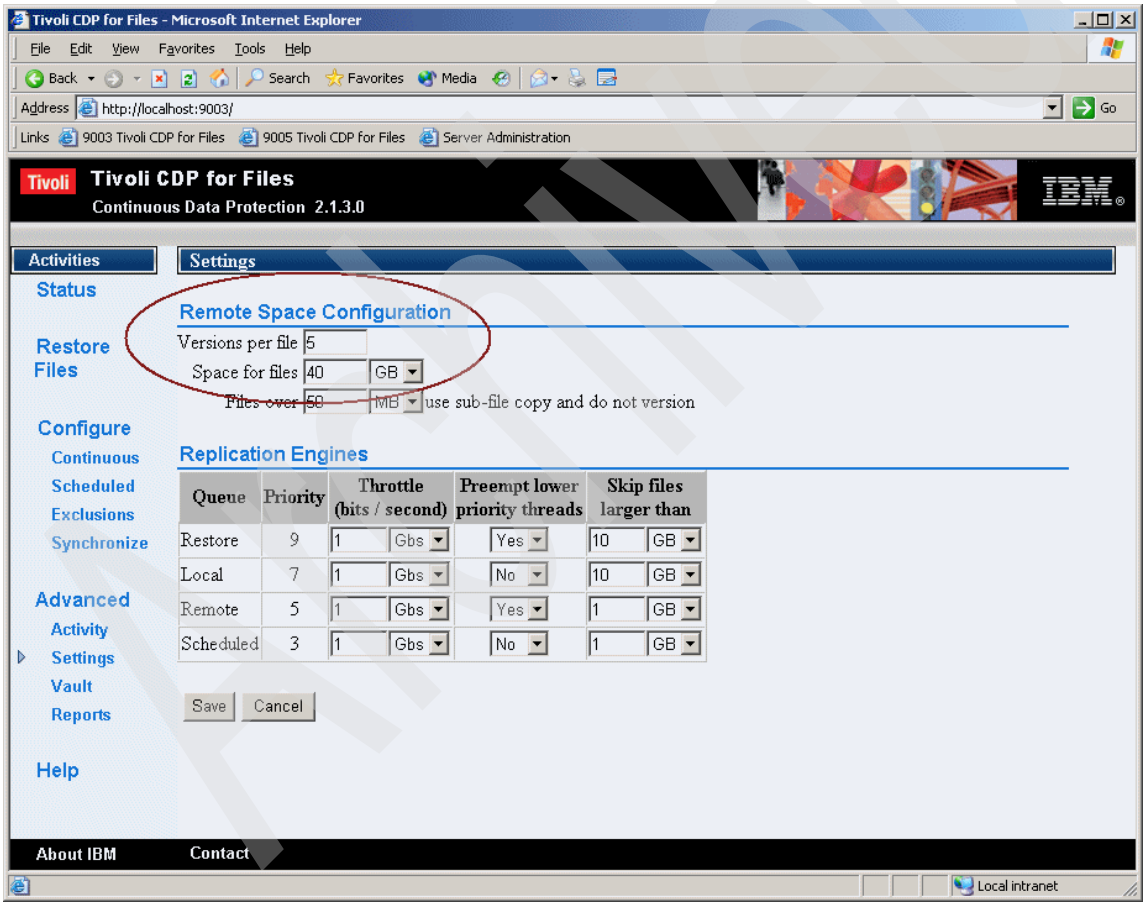


Figure 3-20 Remote Space Configuration settings

Changing drive letters

One of the main features of Windows operating systems in conjunction with USB (storage) devices is the plug-and-play functionality that automatically assigns a drive letter to a USB device as soon as it gets connected to the system. Usually, Windows keeps track of the already assigned drive letters (persistent drive letters) so that the *same device* gets the *same drive letter* assigned when it is plugged in the next time. However, under certain circumstances, this may not hold true, and a newly plugged-in USB device claims the same drive letter as another USB device that is currently offline.

An example is shown in Figure 3-21: the USB disk ("USB_Drive") had been offline when we plugged in an USB stick ("USB_Stick"). The USB stick claimed drive letter (F:) so that the USB disk got the next available drive letter (G:) assigned when we plugged it in later on.

Note: We *did not* change the configuration of Tivoli Continuous Data Protection for Files, so drive (F:) is still defined as the remote backup location (see Figure 3-18 on page 69).

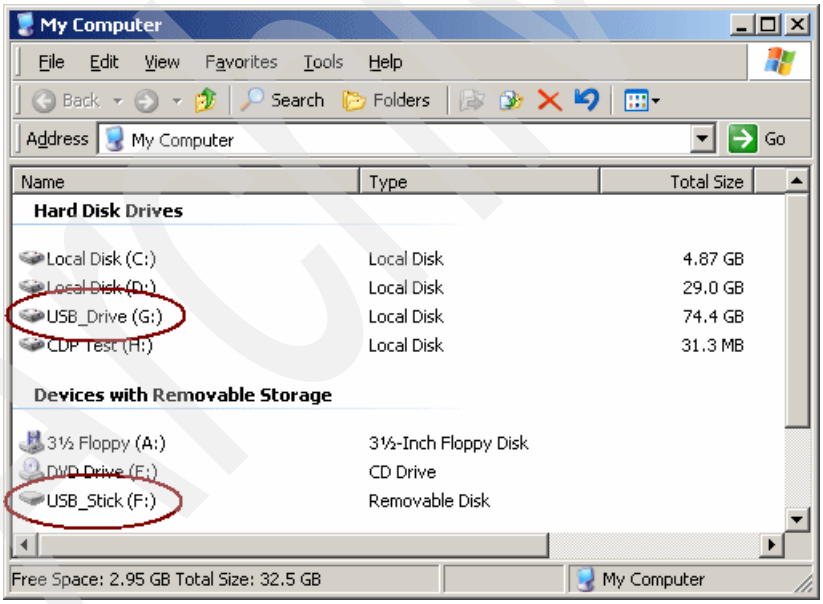


Figure 3-21 Changed drive letter assignments

Important: Tivoli Continuous Data Protection for Files *does not* replicate to the (new) remote location (F:) as long as there is no RealTimeBackup folder on this device. The reason for doing so is to avoid messing up a device that is not meant to be a remote backup location, like a digital camera, for example.

Instead, Tivoli Continuous Data Protection for Files informs you that it cannot reach the target location (Figure 3-22).

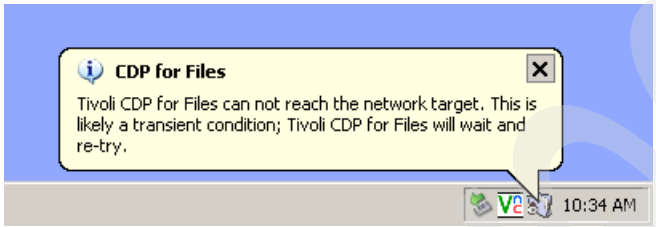


Figure 3-22 Informational message that the network target cannot be reached

In order to avoid unwanted changing of driver letters, you should consider assigning manually your removable disk a drive letter near the end of the alphabet, for example, X, Y or Z, as available drive letters are assigned automatically top-down in the alphabet. It also a good idea to check the drive letter assignments each time you bring new USB devices online and correct them if necessary.

To manually change the driver letter assignment for your external USB drive, please follow these steps:

1. On the Windows desktop, right-click **My Computer** and then click **Manage**.
2. Under Computer Management, click **Disk Management**. In the right pane, you will see your drives listed.
3. Right-click the drive or device you want to change, and then click **Change Drive Letter and Paths**.
4. Click **Change**, click **Assign the following drive letter**, click the drive letter you want to assign, and then click **OK**.
5. Click the **Yes** button when the pop-up window appears asking you to confirm the change of the drive letter.

3.2.2 File server issues

In this section, we will discuss replication problems in case you have decided to protect your files by storing them on a remote network location (file server) for additional protection (either continuously or scheduled).

Note: For avoiding general problems using a file server as a remote backup location, please be aware of the following:

- Log on to your machine with a user name and password that Tivoli Continuous Data Protection for Files can use to authenticate transparently into the network location you have specified. If not, you can alternatively log into the network using another account with regular privileges interactively (for example, by using the **`Net Use`** command).
- Some versions of Windows have a concept of simplified file sharing, which allows one computer to network-attach to another with very little difficulty. The resulting connection allows only limited file system capabilities. If possible, disable simplified file sharing on the target system, as it limits how well Tivoli Continuous Data Protection for Files can produce an identical copy of your files. If simplified file sharing is not disabled, some information, such as access control lists or file streams, may not get copied correctly.

Transient networks

Replication problems due to transient networks can have a variety of different causes. All have the problem in common that the remote location (file server) cannot be accessed over the network and therefore Tivoli Continuous Data Protection for Files fails replicating to this backup target.

Possible reasons, among many, are:

- Your own system is not connected to the network (for example, when you work from home and are not logged on to your company's network).
- The network has a problem (for example, a router/switch/hub is defective).
- The file server is unavailable (for example, due to maintenance work).

If the remote backup location is not reachable when Tivoli Continuous Data Protection for Files tries to replicate to it, you will see the message shown in Figure 3-22 on page 72.

Important: Tivoli Continuous Data Protection for Files *will not* stop keeping track of the changes you make to your files even when you see this message. It will wait for some time and try to replicate the changed files later again, as this may be a transient condition.

Once the file server can be reached again, you will get informed about this event by Tivoli Continuous Data Protection for Files (see Figure 3-23) and replication continues.

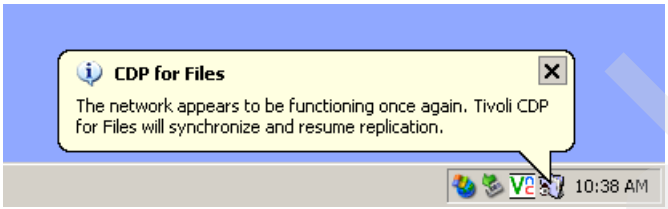


Figure 3-23 Remote location is reachable again and replication continues

Universal Naming Convention (UNC) versus drive letters

To specify a remote backup location in the Tivoli Continuous Data Protection for Files GUI (for continuous backups or scheduled protection), you can either use the Universal Naming Convention (UNC) name of the file server or the drive letter you have it mapped to.

In Figure 3-24, you can see that we connected to a shared network folder e$ on file server Izmir and have mapped it to drive letter (W:).

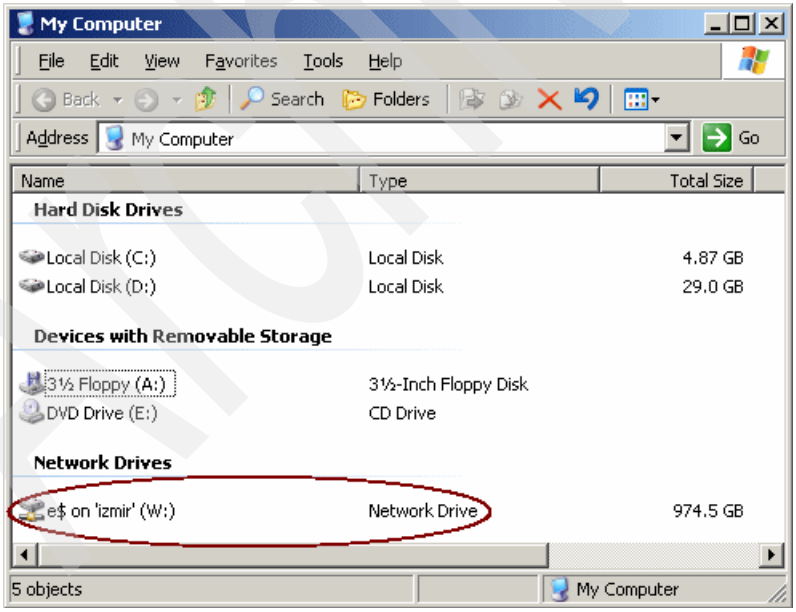


Figure 3-24 Shared network folder e$ on file server Izmir mapped to drive (W:)

Tip: Use the UNC naming specification of the file server instead of drive letters, since drive letters can change after rebooting and many times do not reconnect automatically.

In our case, the recommended way to specify the file server is shown in Figure 3-25 using the UNC name \\izmir\e$ instead of drive letter (W:).

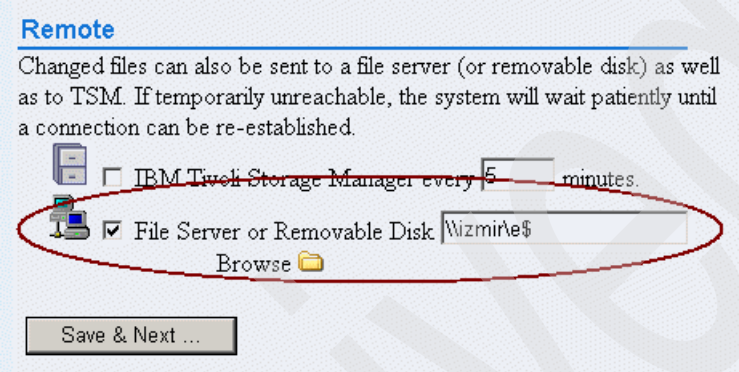


Figure 3-25 Using the UNC name instead of the drive letter

3.3 IBM Tivoli Storage Manager issues

The Tivoli Continuous Data Protection for Files has additional support for protecting files using the IBM Tivoli Storage Manager. To use the TSM for storing files on a remote location, a TSM Backup/Archive client needs to run on the same system as the Tivoli Continuous Data Protection for Files and a TSM server must be available in the network. In this section, we discuss the potential issues related to the Tivoli Continuous Data Protection for Files in conjunction with the TSM Backup/Archive client.

Note: In this section, we do *not* describe in detail how to install and configure the TSM Backup/Archive client with all its available options. For more information about this topic, refer to *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788. We assume that the TSM Backup/Archive client has already been installed successfully on the same system as the Tivoli Continuous Data Protection for Files.

General information

In order to run properly, the IBM Tivoli Storage Manager client needs a client options file (dsm.opt). This file is *not* installed automatically during the TSM Backup/Archive client installation. Instead, the installation process creates a sample client options file called *dsm.smp*. If you accept the default installation path, this file is in the C:\Program Files\Tivoli\TSM\config directory. The dsm.smp file is a generic configuration file that contains communication parameters that are normally used in a Windows environment. You can use this file as a template when customizing your own options file by performing the following steps:

1. Copy the dsm.smp file to your C:\Program Files\Tivoli\TSM\baclient directory.
2. Rename it as dsm.opt.
3. Open this file in Notepad or your favorite plain text editor and customize it for your environment.

One of the most important purposes of the options file is to specify the communication protocol necessary to establish communications between your backup client and the backup server. Use the commmethod option to specify a communication protocol. For example, to use the Transmission Control Protocol (TCP)/Internet Protocol (IP) communication protocol, enter:

```
COMMMethod TCPIP
```

You must also specify the TCP/IP server address of the backup server you want to connect to by using the tcpserveraddress option. For example, you can enter the following:

```
TCPServeraddress tsmserver.yourcompanyname.com
```

You need to replace `tsmserver.yourcompanyname.com` with the valid TCP/IP address of your TSM server. To specify the TCP/IP port on which the TSM server can be reached under this TCP/IP address, use the tcpport option, for example:

```
TCPPort 1500
```

You can also specify what you want to call your workstation by using the nodename option. When you register with the backup server during setup, this is the name the server uses for your workstation. If you do not specify a node name, the server identifies your workstation by its host name. You can type the host name at a command prompt to see your workstation's host name, for example:

```
NODename tsmclient
```

If your TSM administrator decides that each client node needs to authenticate itself to the server when starting a session, you need to specify one of the following:

- If you want to be prompted for a password (PASSWORDAccess prompt).
- If the TSM Backup/Archive client automatically generates a new password for your client node each time it expires and stores the password encrypted in the Windows registry (PASSWORDAccess generate).

Table 3-1 lists the most important options of the TSM Backup/Archive client options file, and provides a short description of each of them and their default value (if applicable).

Table 3-1 Example of the most important options of dsm.opt

Option	Description	Default value (if not set)
COMMMethod	This option specifies the communication method you use to provide connectivity for client-server communication.	TCPip
TCPServeraddress	This option specifies the TCP/IP address for a TSM server. You can obtain this server address from your administrator.	none (Must be explicitly specified.)
TCPPort	This option specifies a TCP/IP port address for a TSM server. You can obtain this address from your administrator.	1500
NODename	Use this option in your client options file dsm.opt to identify your workstation to the server. You can use different node names to identify multiple operating systems on your workstation.	workstation (host) name
PASSWORDAccess	This option specifies whether you want to generate your password automatically or set it as a user prompt. Your administrator can require a password for your client node by enabling the authentication feature. Ask your administrator if a password is required for your client node.	prompt

Figure 3-26 shows the dsm.opt file we used in our lab.

```
COMMMethod          TCPip
TCPServeraddress    florence
TCPPort             1500
NODename            CAIRO_WS
PASSWORDAccess      generate
```

Figure 3-26 The dsm.opt file as used in our lab

Tip: If you have configured the Tivoli Continuous Data Protection for Files using the IBM Tivoli Storage Manager *for the first time*, we recommend that you perform one of the following actions:

- Log off and log on again if you are running the Tivoli Continuous Data Protection for Files as a logged-in application (default).
- Restart the CDP for Files service if the Tivoli Continuous Data Protection for Files is running as a Windows service.

For more details, see “Logging off / logging on and restarting the service” on page 64.

3.3.1 Missing IBM Tivoli Storage Manager client options file (dsm.opt)

If you have configured the Tivoli Continuous Data Protection for Files using the IBM Tivoli Storage Manager client, the Tivoli Continuous Data Protection for Files will start the TSM Backup/Archive command-line client (dsmc.exe) in the background in either of the following scenarios:

- If the period you specified in your continuous configuration has expired (continuous protection)
- If it is time for a scheduled backup (scheduled protection)

Notes:

- The Tivoli Continuous Data Protection for Files starts the TSM Backup/Archive client only if there is work to do, that is, if the files for continuous protection have been created, modified, or deleted since the last backup.
- For determining the time when the TSM Backup/Archive client needs to be invoked, the Tivoli Continuous Data Protection for Files uses an internal schedule mechanism (not the Windows or the TSM Backup/Archive client scheduler service).

In our example, we specified a period of five minutes (see Figure 3-27).

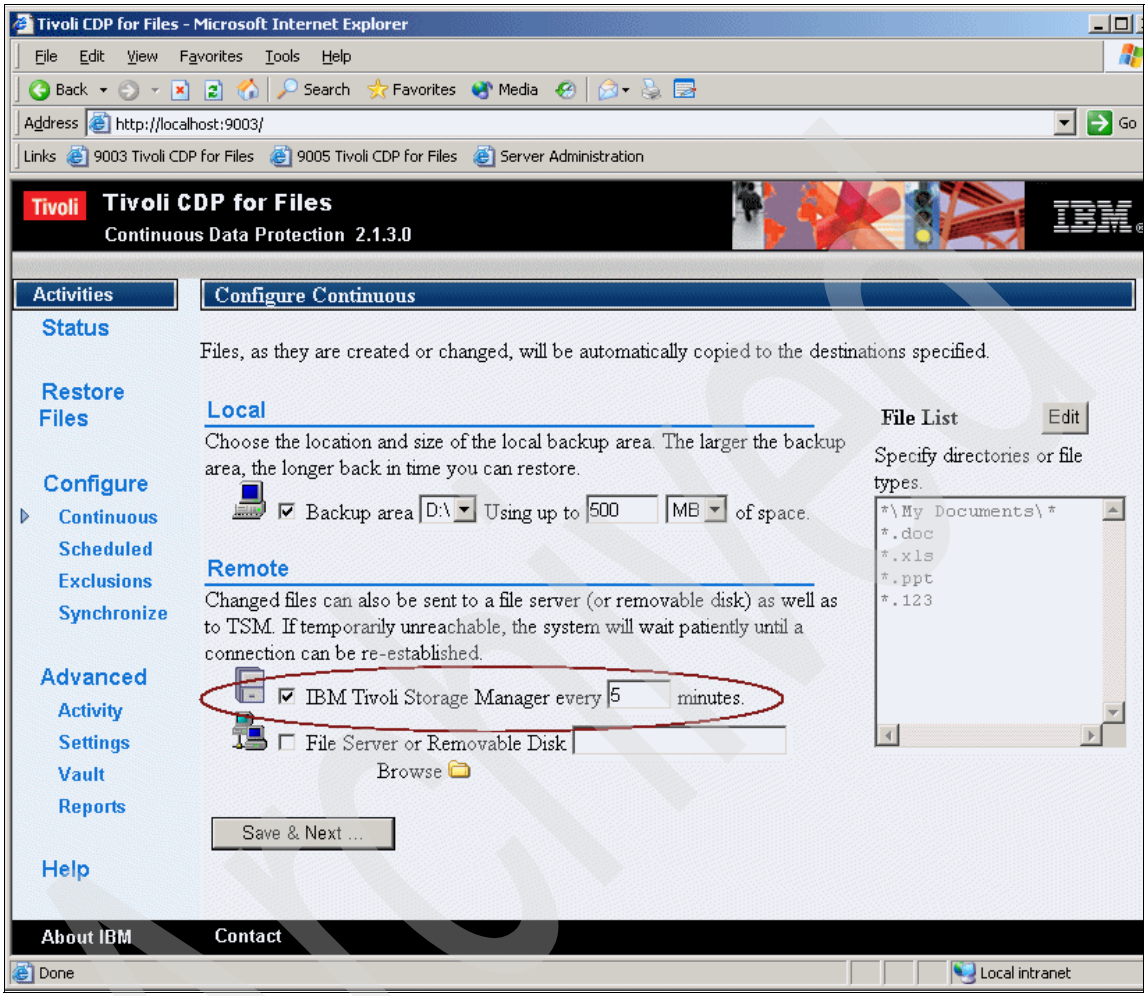


Figure 3-27 Continuous protection using the TSM every five minutes

Note: For more details about how Tivoli Continuous Data Protection for Files works together with the IBM Tivoli Storage Manager, and the command-line options that are passed over to the TSM Backup/Archive client when it is started, refer to 2.1.5, “IBM Tivoli Storage Manager integration” on page 25.

If the dsm.opt is missing in the C:\Program Files\Tivoli\TSM\baclient directory because it has not yet been created, moved somewhere else, deleted, or renamed, the TSM Backup/Archive client will not start, as it cannot find the necessary client options file.

If this happens when the Tivoli Continuous Data Protection for Files invokes the TSM Backup/Archive client, a warning message appears in the notification area in the upper right corner, as shown in Figure 3-5 on page 57. This message informs you that the Tivoli Continuous Data Protection for Files is experiencing a problem and requests you to check the system event log for more details.

When you open the Windows Event Viewer, as described in “Windows system event log” on page 57, you will see two error entries in the system event log from source CDP for Files. Figure 3-28 shows the first of these error entries in the event log.

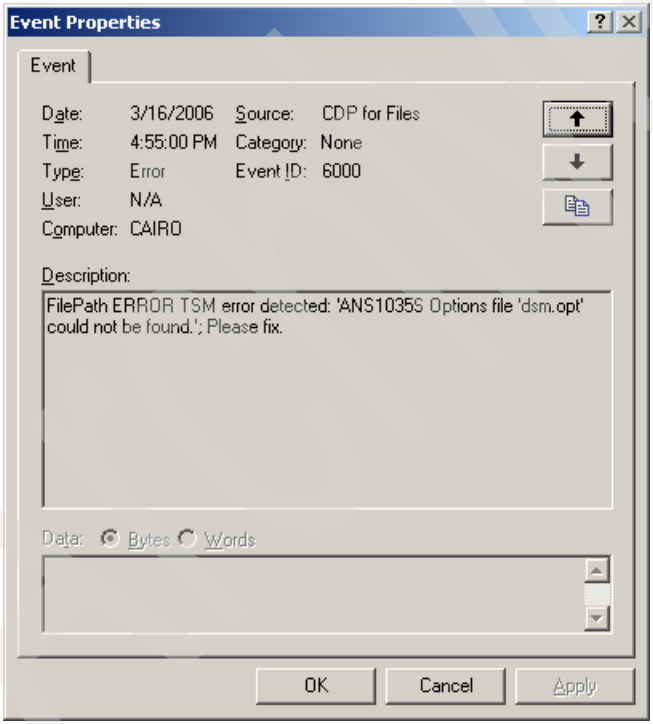


Figure 3-28 Error “ANS1035S Options file dsm.opt not found” in the event log

Figure 3-29 on page 81 shows the filePath error entry in the event log.

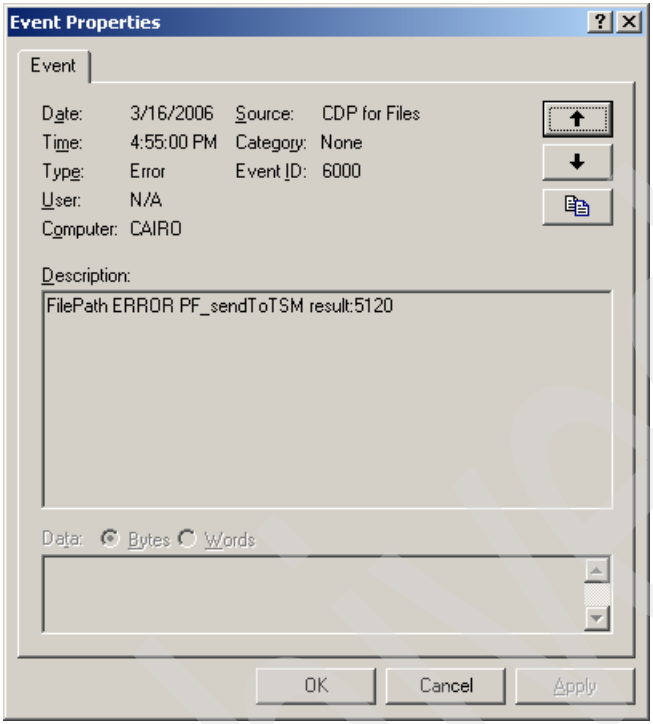


Figure 3-29 FilePath error entry in the system event log

Additionally, two files are created in the C:\Program Files\Tivoli\CDP_for_Files directory: TSMout.log and TSMout.log_acp. Both files contain the same information (see Figure 3-30) as already seen in the first error event log entry (Figure 3-28 on page 80).

```
ANS1035S Options file 'dsm.opt' could not be found.
```

Figure 3-30 Contents of the files TSMout.log and TSMout.log_acp (ANS1035S)

To solve this kind of problem, ensure that a valid and usable file dsm.opt exists in the C:\Program Files\Tivoli\TSM\baclient directory. If necessary, create a new dsm.opt file using the sample option file dsm.smp, as described earlier in this section.

3.3.2 Passwordaccess generate versus passwordaccess prompt

As outlined in Table 3-1 on page 77, one important option in the IBM Tivoli Storage Manager client options file (dsm.opt) is the PASSWORDAccess option. It determines whether you are prompted for the password each time you start a TSM session (PASSWORDAccess prompt) or if the password is stored encrypted in the Windows registry and is taken automatically from there without prompting you for it (PASSWORDAccess generate).

In order to use the TSM Backup/Archive client from within the Tivoli Continuous Data Protection for Files, you have to set the PASSWORDAccess generate option. The reason for this is that the Tivoli Continuous Data Protection for Files invokes the TSM Backup/Archive command-line client under the surface and invisible to the user. If you have set the PASSWORDAccess prompt option, the TSM Backup/Archive client immediately prompts you to enter a user ID and password after it has started. As this process runs in the background without opening a real window for entering responses to the TSM Backup/Archive client or for issuing TSM Backup/Archive client commands, it stays active as a Windows process waiting for you to enter a user ID and password, which cannot be done in this case.

The following section describes the symptoms you see if you do not use the PASSWORDAccess generate option. In our example, we use the TSM Backup/Archive client as one possibility for continuous data protection by sending high-importance files to a TSM server every five minutes (see Figure 3-27 on page 79).

When you open the GUI of the Tivoli Continuous Data Protection for Files (either by double-clicking the Tivoli Continuous Data Protection for Files icon in the notification area in the upper right corner or by opening an Internet browser and entering the URL `http://localhost:9003`), you will see, by default, the status window including the summary information for continuous and scheduled protection. As soon as you create, modify, rename, or delete a high-importance file for continuous data protection, you see the number of pending actions for the TSM in the continuous protection area increasing (see Figure 3-31 on page 83).

This number should revert back to 0 (zero) as soon as the Tivoli Continuous Data Protection for Files starts the TSM Backup/Archive client and the outstanding actions can be executed successfully by:

- Sending the file to the TSM server if it has been created or modified.
- Expiring the file on the TSM server if it has been deleted or renamed.

In case the number of pending actions does not decrease after the period to start the TSM Backup/Archive client has elapsed, the most likely reason for this is that

the TSM Backup/Archive client has problems in either starting or connecting successfully to the TSM server.

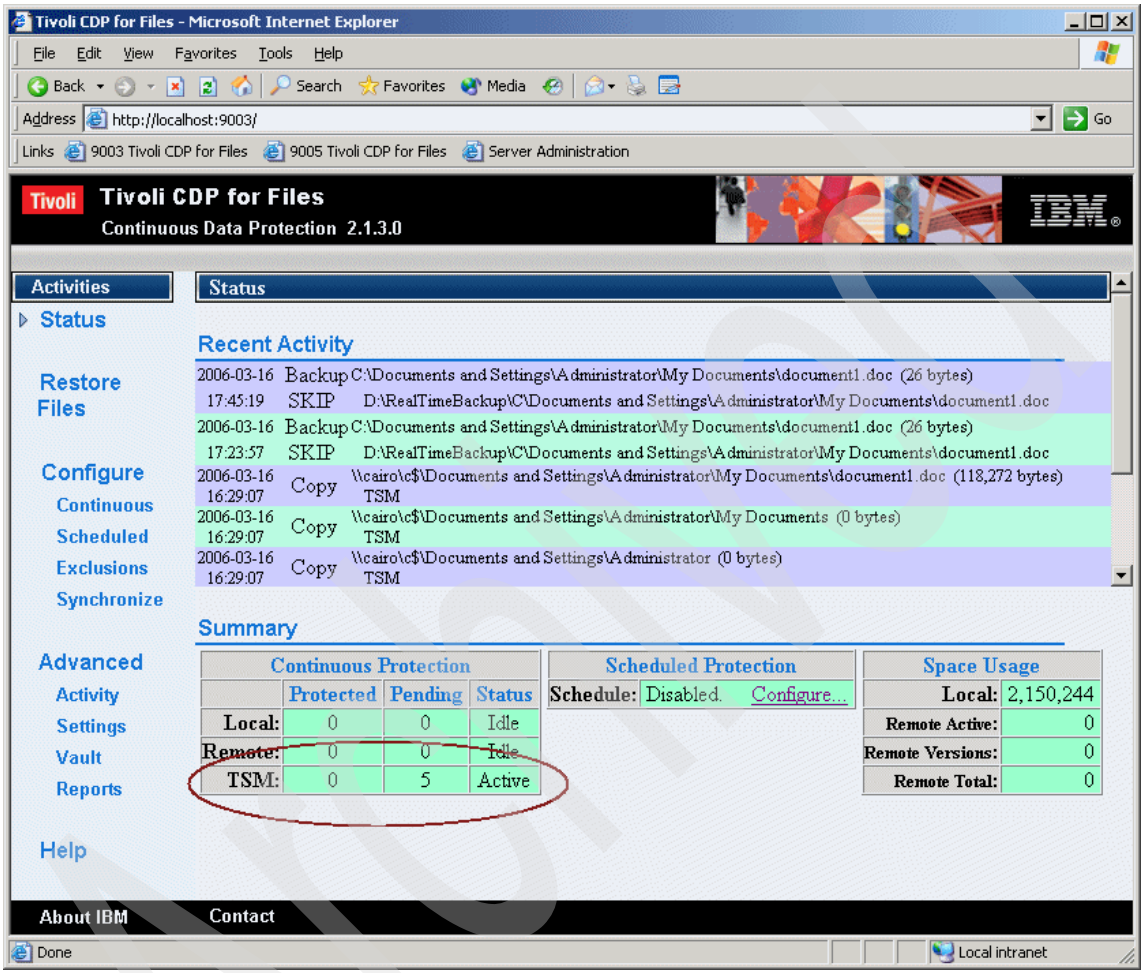


Figure 3-31 Pending activities for the IBM Tivoli Storage Manager

If this happens, you should check the Windows Task Manager to see if the TSM Backup/Archive command-line client process dsmc.exe is running and hanging in the background. To do this, follow these steps:

1. Right-click the Windows Taskbar and select **Task Manager**.
2. Click the **Processes** tab to show the active (running) processes.

3. Locate the dsmc.exe process in the left column named *Image Name* (see Figure 3-32).

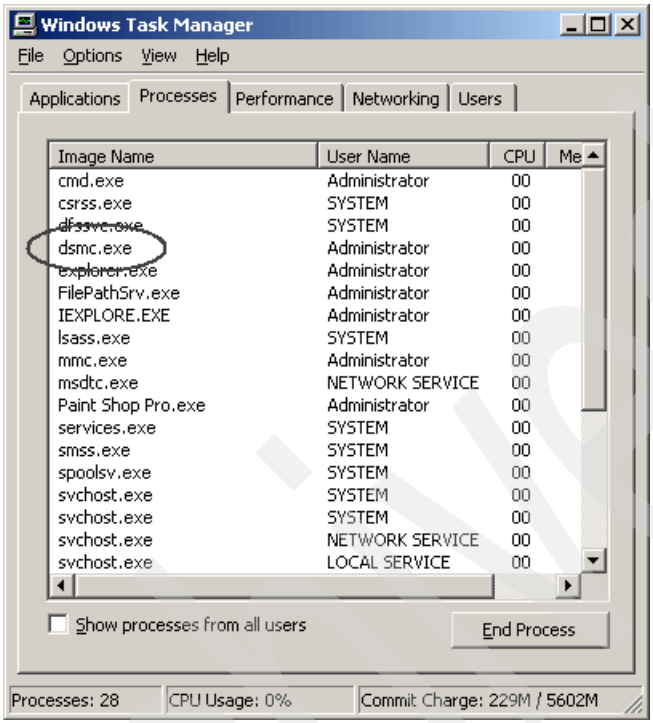


Figure 3-32 The TSM Backup/Archive client process dsmc.exe in the Windows Task Manager

If you locate the dsmc.exe process in the process list with a CPU usage of 0% and the number of pending actions for the TSM has not decreased, this is an indication of an issue with either the TSM Backup/Archive client itself or in connection with the TSM server. As you can see, the Tivoli Continuous Data Protection for Files is able to start the TSM Backup/Archive client due to the active TSM Backup/Archive client process.

Note: At this time, you will *not* see any error message from the Tivoli Continuous Data Protection for Files indicating any problems with the IBM Tivoli Storage Manager.

To exit this situation, first cancel the dsmc.exe process:

1. Right-click **dsmc.exe** and select **End Process** (see Figure 3-33).

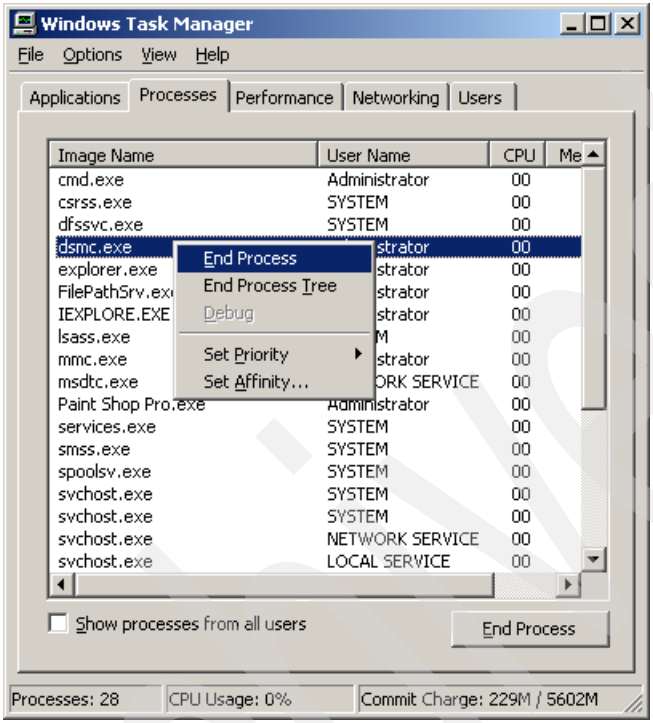


Figure 3-33 Ending the dsmc.exe process

2. When you terminate a process, a warning message appears from the Windows Task Manager (Figure 3-34) informing you about the possible consequences.

   Click **Yes** to the question whether you are sure you want to terminate the process. This cancels the dsmc.exe process.

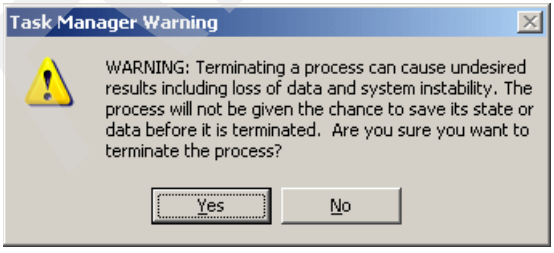


Figure 3-34 Warning message when terminating the dsmc.exe process

As soon as you have canceled the dsmc.exe process, the Tivoli Continuous Data Protection for Files issues an informational message in the notification area of the taskbar, as shown in Figure 3-35. It informs you about the inability of the system to connect properly to the TSM server.

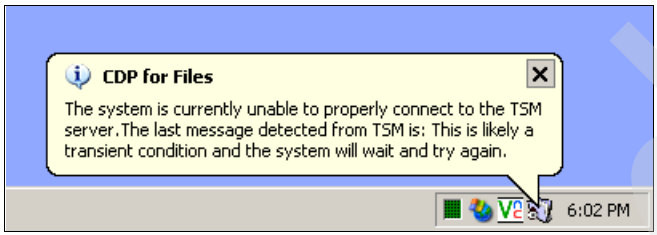


Figure 3-35 The Tivoli Continuous Data Protection for Files information message

At the same time, when you open the Event Viewer (as described in "Windows system event log" on page 57), you see two event entries (one error and one informational event entry) from the source CDP for Files in the Windows system event log. Figure 3-36 shows the error entry.

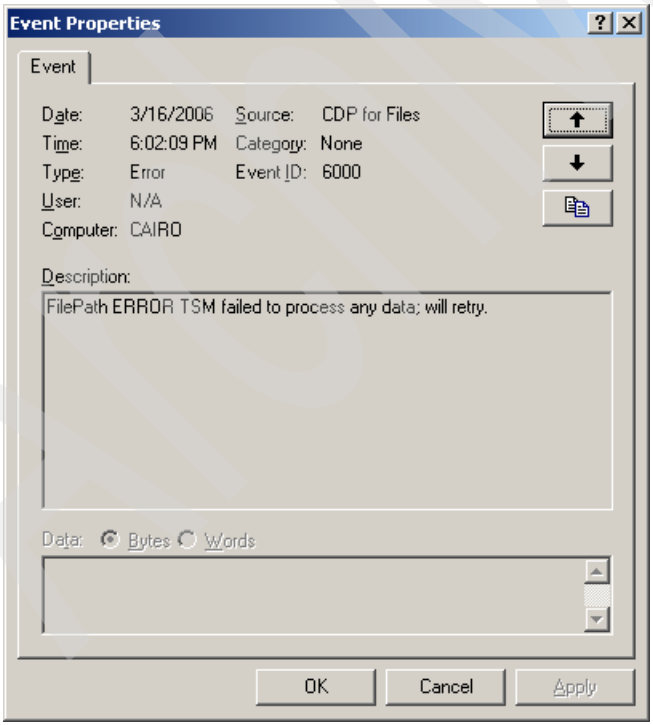


Figure 3-36 "TSM failed to process any data" error entry in the system event log

Figure 3-37 shows the informational event entry.

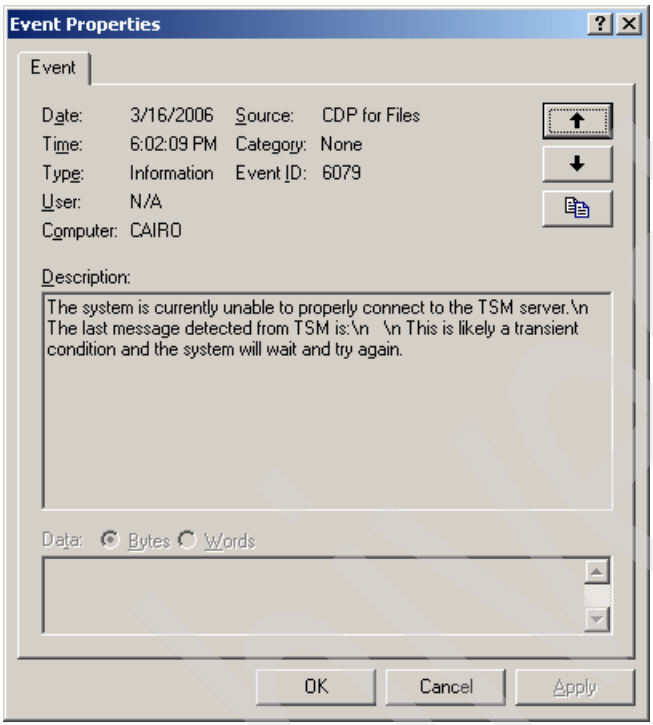


Figure 3-37 Informational message in the system event log due to connection problems with the TSM server

At this point, you should check the contents of the file dsm.opt in your C:\Program Files\Tivoli\TSM\baclient directory and see if you have specified the PASSWORDAccess option and check the value you set for it. Figure 3-38 shows the dsm.opt file we have used.

```
COMMMethod          TCPip
TCPServeraddress    florence
TCPPort             1500
NODename            CAIRO_WS
```

Figure 3-38 File dsm.opt without the PASSWORDAccess option

As you can see, we did not specify the PASSWORDAccess option, so the default PASSWORDAccess prompt is used by the TSM Backup/Archive client (see Table 3-1 on page 77). This is causing the problem here in this example, as the TSM Backup/Archive command-line client was started in the background waiting for you to enter a user ID and password. As you cannot enter the required user ID and password for this background process, the TSM Backup/Archive command-line client does not connect to the TSM server.

You need to add the `PASSWORDAccess generate` option to your dsm.opt file. This can be done by editing dsm.opt with the Notepad editor:

1. Select **Start** → **Run**, type **`notepad`**, and click **OK**. This opens the Notepad editor.
2. Click **File** → **Open**, and select **All Files** in the drop-down list named Files of type.
3. Navigate to the C:\Program Files\Tivoli\TSM\baclient directory by using the main navigation window in the middle of the window.
4. Locate the dsm.opt file and select it.
5. Click the **Open** button. The dsm.opt file now appears in Notepad.
6. Add a new line with `PASSWORDAccess generate`.
7. Click **File** → **Exit**, and click **Yes** to the question whether you want to save the changes.

The dsm.opt file now looks like Figure 3-39.

```
COMMMethod          TCPip
TCPServeraddress    florence
TCPPort             1500
NODename            CAIRO_WS
PASSWORDAccess      generate
```

Figure 3-39 File dsm.opt with PASSWORDAccess generate option

Once the TSM client option `PASSWORDAccess generate` has been set, you need to manually start the TSM Backup/Archive command-line client or GUI at least one time again to enter the user ID and password, which then will be stored encrypted into the Windows registry.

To manually start the TSM Backup/Archive command-line client, please do the following:

1. Select **Start** → **Run**, type **`cmd`**, and click **OK**. A Windows command-line window appears.

2. To change to the installation directory of the TSM Backup/Archive client, enter **cd “\program files\tivoli\tsm\baclient”**.
3. To start the TSM Backup/Archive command-line client, enter **dsmc**.

   If this is the first time you have used the TSM Backup/Archive command-line client with option `PASSWORDAccess generate`, you will be prompted (a last time) to enter a user ID and password for node name CAIRO_WS.

   This will then store the entered password encrypted into the Windows registry from where it will be taken each time you start the TSM Backup/Archive client with the `PASSWORDAccess generate` option, without prompting you for a user ID and password again.
4. When prompted for your user ID, type CAIRO_WS or just press Enter.
5. When prompted for your password, type the password for the user ID (node name) and press Enter.
6. To stop the TSM Backup/Archive command-line client again, use the **quit** command.
7. To close the Windows command-line window, type **exit**.

Figure 3-40 shows an example of such a TSM Backup/Archive command-line client session.

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\program files\tivoli\tsm\baclient"

C:\Program Files\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 3, Level 2.0
  Client date/time: 03/20/2006 18:48:20
(c) Copyright by IBM Corporation and other(s) 1990, 2005. All Rights Reserved.

Node Name: CAIRO_WS
Please enter your user id <CAIRO_WS>: CAIRO_WS

Please enter password for user id "CAIRO_WS": ********

Session established with server FLORENCE: Windows
  Server Version 5, Release 3, Level 2.0
  Server date/time: 03/20/2006 18:47:35  Last access: 03/20/2006 18:47:12

tsm> quit

C:\Program Files\Tivoli\TSM\baclient>
```

Figure 3-40 TSM Backup/Archive command-line client session

Alternatively, you can use the TSM Backup/Archive client GUI using one of the following methods:

- Click the Windows **Start** button and select **Programs** → **Tivoli Storage Manager** → **Backup Archive GUI**.
- Click the Windows **Start** button and select **Run**, enter the full path to the TSM Backup/Archive client GUI executable file (dsm.exe), and click **OK**.
- On a Windows command line, change the directory to the TSM installation directory and enter **dsm**.

If the TSM Backup/Archive client GUI (see Figure 3-41 on page 91) starts without opening a pop-up window prompting you for a password to log in to the TSM server, everything is fine, as the password has been taken from the Windows registry.

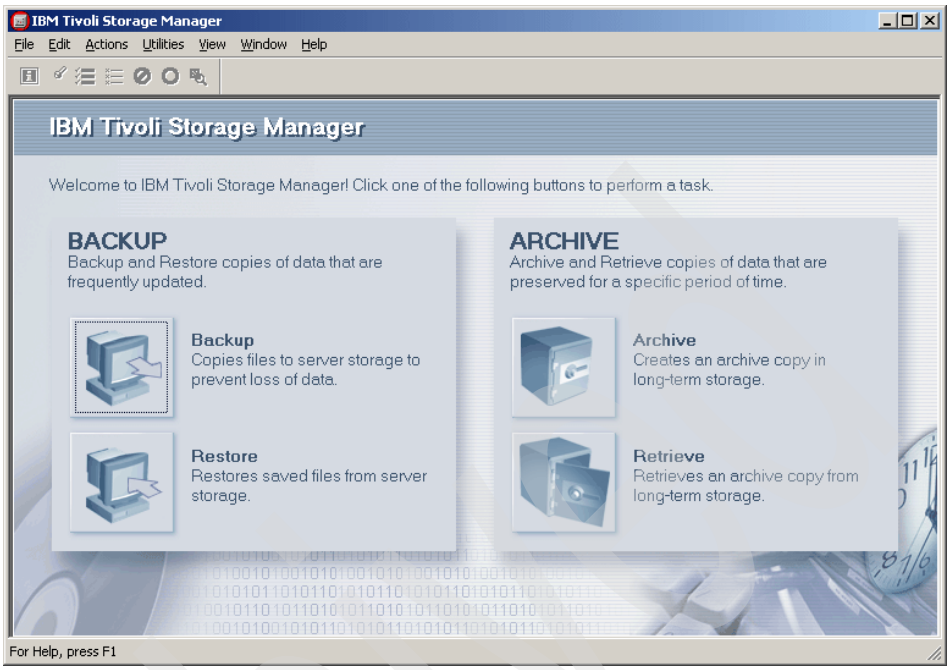


Figure 3-41 TSM Backup/Archive client GUI

Now that we have verified that the PASSWORDAccess generate option has been set and used correctly, the next time when the Tivoli Continuous Data Protection for Files starts the TSM Backup/Archive client, it can communicate with the TSM server (assuming the TSM server is up and running). Figure 3-42 shows the informational message from the Tivoli Continuous Data Protection for Files informing you about the successful communication with the TSM server again.

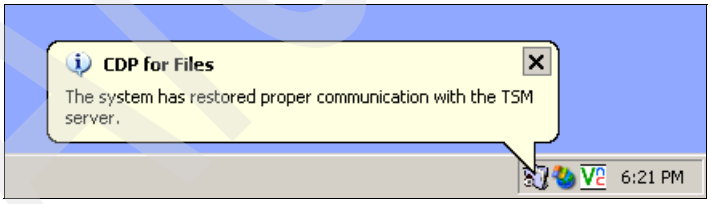


Figure 3-42 Successful communication with the TSM server

The same information seen in Figure 3-42 is reported in an informational event entry for the CDP for Files source in the system event log.

You can check the success of the proper communication between the TSM Backup/Archive client and the TSM server in the status window of the Tivoli

Continuous Data Protection for Files GUI. There are no more pending actions for the TSM in the continuous protection area and the number has reverted back to 0 (zero). Instead, the number of protected files has increased (see Figure 3-43).

Figure 3-43 The number of files protected by the TSM

Attention: Due to the way the Tivoli Continuous Data Protection for Files works, the number of pending actions for the TSM continuous protection *does not* necessarily mean the same as the number of files that are protected by the TSM. For more information, refer to 2.1.5, “IBM Tivoli Storage Manager integration” on page 25.

3.3.3 IBM Tivoli Storage Manager client option Subdir Yes not valid

Table 3-1 on page 77 shows the most important IBM Tivoli Storage Manager (TSM) client options to get the TSM Backup/Archive client to run at a basic level. There are many other options you can use in the TSM Backup/Archive client options file (dsm.opt) to adjust the behavior of the TSM Backup/Archive client to fit your needs. For all possible options, refer to Chapter 9, “Using processing options”, in *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788.

One of these TSM Backup/Archive client options is the SUbdir option. Table 3-2 provides a short description and the default value for the SUbdir option, if is not explicitly set in the TSM Backup/Archive client options file dsm.opt.

Table 3-2 Explanation of TSM Backup/Archive client option SUbdir

Option	Description	Default value (if not set)
SUbdir	This option specifies whether you want to include subdirectories of named directories for processing.	No

If you want to include the subdirectories for processing when backing up a specific path and file using your TSM Backup/Archive client, you have to set the SUbdir Yes option in the dsm.opt file. Then the dsm.opt looks like the one shown in Figure 3-44.

```
COMMMethod          TCPip
TCPServeraddress    florence
TCPPort             1500
NODename            CAIRO_WS
PASSWORDAccess      generate
SUbdir              Yes
```

Figure 3-44 File dsm.opt using the SUbdir Yes option

Attention: To run the TSM Backup/Archive client together with the Tivoli Continuous Data Protection for Files (that is, the Tivoli Continuous Data Protection for Files starts the TSM Backup/Archive command-line client dsmc.exe), the Subdir Yes option is *not mandatory*. It *can* be used, for example, if you are using the IBM Tivoli Storage Manager as a separate (second) backup solution for your system beside the Tivoli Continuous Data Protection for Files, and you want to include the subdirectories for backup processing in this specific combination.

If you set Subdir Yes in dsm.opt and the Tivoli Continuous Data Protection for Files starts the TSM Backup/Archive command-line client, you will see an `ANS1891W` warning message in the TSM Backup/Archive client error file (dsmerror.log), as shown in Figure 3-45.

```
03/21/2006 13:39:57 ANS1891W SUBDIR is not a valid option when using
FILELIST, SUBDIR will be ignored.
```

Figure 3-45 Entry in the dsmserror.log due to SUbdir Yes being used in dsm.opt

Tip: TSM Backup/Archive client error and warning messages are written to the error log file dsmerror.log, or the file you specify with the errorlogname option in the dsm.opt file. The dsmerror.log file resides in the directory you set with the DSM_LOG environment variable or in the installation directory of the TSM Backup/Archive client. The dsmerror.log file is a good source to start problem determination, and you should check this first if you have any kind of problem with the TSM Backup/Archive client.

The reason for the warning message `ANS1891W SUBDIR is not a valid option when using FILELIST, SUBDIR will be ignored` is because of the way the Tivoli Continuous Data Protection for Files invokes the TSM Backup/Archive client.

The Tivoli Continuous Data Protection for Files starts dsmc.exe by using a TSM Backup/Archive command-line option named filelist, specifying the location and the name of the file containing the list of files to process with the command. When the filelist option is specified on the TSM Backup/Archive command line, the subdir option is not a valid option and, therefore, will be ignored (see option filelist in Chapter 9, “Using processing options”, in *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788.

The backup of the files is not influenced by the `ANS1891W` warning message itself and, therefore, you can safely disregard this message.

Note: Refer to 2.1.5, “IBM Tivoli Storage Manager integration” on page 25 for more information about how the Tivoli Continuous Data Protection for Files works together with the IBM Tivoli Storage Manager.

3.3.4 Conflicting include/exclude lists

Both the Tivoli Continuous Data Protection for Files and the IBM Tivoli Storage Manager (TSM) manage files or directories for backup services based on include/exclude lists. This can lead to potential conflicts between the Tivoli Continuous Data Protection for Files and the IBM Tivoli Storage Manager, for example, if a file is included in the Tivoli Continuous Data Protection for Files for continuous protection but is excluded by the TSM Backup/Archive client from being stored on the TSM server.

Note: For details about how to include files, directories, or both for protection, or how to exclude them from protection in the Tivoli Continuous Data Protection for Files, refer to 2.1.3, “Directories and files” on page 20.

By design, the IBM Tivoli Storage Manager backs up any file that is not (explicitly) excluded. This can be done either in the TSM client options file (dsm.opt) or on the TSM server (for multiple TSM clients together) using a client option set. We do not discuss the latter option here. For more information about defining a client option set, refer to Chapter 5, “Administrative Commands”, in *IBM Tivoli Storage Manager for Windows Administrator’s Reference*, GC32-0783.

There is no predefined exclude list available in dsm.opt, therefore, you have to create this file. In this case, *all files* are considered to be backed up. We do not recommend this, as it will also include, for example, the Windows system files, such as the paging file (pagefile.sys) for backups, or the temporary Internet files, which are not really useful. A minimum exclude list for the TSM Backup/Archive client is shown in Figure 3-46 on page 96.

Besides this exclude list, you can add various types of include or exclude statements into the dsm.opt file. By doing this, you can create an include or exclude list that exactly fits your special needs for files that are backed up in your environment, and for those that are not backed up. For full details about possible include/exclude statements and their syntax, refer to Chapter 2, “Configuring Tivoli Storage Manager”, in *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788.

```
*
* Example minimum TSM exclude list
*
Exclude "*:\microsoft uam volume\...\*"
Exclude "*:\microsoft uam volume\...\*.*"
Exclude *:\...\pagefile.sys
Exclude *:\MSDOS.SYS
Exclude *:\IO.SYS
Exclude *:\...\system32\config\...\*
Exclude *:\...\system32\Perflib*.dat
Exclude *:\...\system32\dhcp\...\*
Include *:\...\system32\dhcp\backup\...\*
Exclude *:\...\system32\dns\...\*
Include *:\...\system32\dns\backup\...\*
Exclude.dir "*:\System Volume Information"
Exclude.dir "*:\...\Temporary Internet Files"
Exclude.dir *:\Recycled
Exclude.dir *:\Recycler
```

Figure 3-46 Example of a minimum exclude list for the TSM Backup/Archive client

But adding include/exclude statements in dsm.opt may also lead to conflicts with the include/exclude list of the Tivoli Continuous Data Protection for Files. As shown in our configuration example in Figure 3-27 on page 79, we defined all files with extension *xls* (Microsoft Excel files) as high-importance files. These files are protected continuously by the Tivoli Continuous Data Protection for Files and stored locally on our D drive as well as sent to the TSM server every five minutes.

Figure 3-47 shows the file dsm.opt we use in this example. Note that we added an exclude statement (`Exclude "*:\...\*.xls"`), which excludes all files with extension xls from being backed up by the TSM Backup/Archive client.

```
COMMMethod         TCPip
TCPServeraddress   florence
TCPPort            1500
NODename           CAIRO_WS
PASSWORDAccess     generate

Exclude "*:\...\*.xls"
```

*Figure 3-47 File dsm.opt with exclude statement for *.xls files*

If we edit our sample file file.xls under the directory C:\Documents and Settings\Administrator\My Documents and save the changes, this leads to two events:

- The Tivoli Continuous Data Protection for Files immediately stores the changed file file.xls in the local backup area.

  This event works.

- After five minutes, the Tivoli Continuous Data Protection for Files starts the TSM Backup/Archive client to send the changed file file.xls to the TSM server for continuous remote protection.

  The latter event fails (that is, the changed file file.xls *is not* sent to the TSM server). This is because we excluded all files ending with xls from being backed up by the TSM Backup/Archive client according to our exclude statement in the dsm.opt file. Instead, a warning message is written into the TSM Backup/Archive client error log file dsmerror.log (see Figure 3-48) informing you about this failure.

```
03/23/2006 11:00:57 ANS1115W File '\\cairo\c$\Documents and
Settings\Administrator\My Documents\file.xls' excluded by Include/Exclude
list
```

Figure 3-48 ANS1115W warning message in dsmerror.log (excluded file)

Attention: Files excluded from backup by a IBM Tivoli Storage Manager include/exclude list *will not* be sent to the TSM server even if they are included for protection in the Tivoli Continuous Data Protection for Files.

In order to avoid such include/exclude conflicts between the Tivoli Continuous Data Protection for Files and the IBM Tivoli Storage Manager, you should periodically check the TSM Backup/Archive client error log file dsmerror.log for any `ANS1115W File excluded by Include/Exclude list` messages. If necessary, adjust the include/exclude list of your TSM Backup/Archive client accordingly, so you can be sure that all the files protected by the Tivoli Continuous Data Protection for Files are also stored successfully on the TSM server.

3.3.5 Files containing named streams (Alternate Data Streams)

The New Technology File System (NTFS) allows files to contain multiple *streams* of data, which is why this feature is sometimes also referred to as *Alternate Data Streams* (ADS).

Note: There are many resources for information about file streams and ADS available on the Internet. Details about how to create file streams, how to manipulate them, or how they can be detected is beyond the scope of this chapter, and is therefore not discussed.

For details about file streams, refer to the following:

- "A Programmer's Perspective on NTFS 2000 Part 1: Stream and Hard Link", on the Microsoft Developer Network (MSDN®) at:

  `http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnfiles/html/ntfs5.asp`

- "How To Use NTFS Alternate Data Streams" in the Microsoft Knowledge Base Article 105763 at:

  `http://support.microsoft.com/kb/105763/en-us`

ADS can be used by the operating system to store additional information in a file. For example, they are used in Windows 2000 and Windows XP to store thumbnails (small/little previews of larger pictures), or to save metadata, such as the identity of the user account that created the file, the title, or search keywords of a file. By using ADS, you can fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities, such as the **`dir`** command or the Windows Explorer.

As ADS are (almost completely) hidden to the operating system, this causes a problem if the files to be monitored for protection have named streams, and when they are passed over to the TSM Backup/Archive client by the Tivoli Continuous Data Protection for Files.

In this section, we demonstrate what appears in the Tivoli Continuous Data Protection for Files and the TSM Backup/Archive client log files in case a file contains a named stream, and the file is eligible for continuous data protection in conjunction with the IBM Tivoli Storage Manager.

To demonstrate this, we create a named stream STREAMNAME with the content STREAMCONTENT for file file.xls. The details are as follows:

- Directory name: C:\Documents and Settings\Administrator\My Documents
- File name: file.xls
- Stream name: STREAMNAME
- Stream content: STREAMCONTENT

Figure 3-49 shows that the named stream STREAMNAME is *not visible* to the operating system using the **dir** command on file file.xls. The same is true if you use the Windows Explorer to list the files in the C:\Documents and Settings\Administrator\My Documents directory.

```
C:\Documents and Settings\Administrator\My Documents>dir file.xls
 Volume in drive C has no label.
 Volume Serial Number is FCBE-5775

 Directory of C:\Documents and Settings\Administrator\My Documents

03/22/2006  11:08 AM         2,031,616 file.xls
               1 File(s)      2,031,616 bytes
               0 Dir(s)     644,861,952 bytes free

C:\Documents and Settings\Administrator\My Documents>more < file.xls:STREAMNAME
STREAMCONTENT

C:\Documents and Settings\Administrator\My Documents>
```

Figure 3-49 Content (STREAMCONTENT) of a named stream (STREAMNAME)

As you can see, the content STREAMCONTENT of the named stream STREAMNAME can be made visible if we enter the **more < file.xls:STREAMNAME** command.

Depending on whether you copy a file containing named streams, or whether you edit it and save the changes you made, the messages (as seen in the TSM Backup/Archive client error log (dsmerror.log)) vary.

Note: The following sections mention a couple of different Tivoli Continuous Data Protection for Files logs. Please refer to Section 3.4, “Log files and FPcommand.bat” on page 108 about their meaning and where they can be found on your Windows system.

Copying a file with named streams

When you copy a file containing a named stream, for example, file file.xls, you will see the messages `ANS1228E Sending of object failed`, `ANS4005E File not found`, and `ANS1804E Selective Backup finished with failures` in the dsmerror.log file, as shown in Figure 3-50.

```
03/22/2006 13:58:22 ANS1228E Sending of object '\\cairo\c$\Documents and
Settings\Administrator\My Documents\file.xls:STREAMNAME' failed
03/22/2006 13:58:22 ANS4005E Error processing '\\cairo\c$\Documents and
Settings\Administrator\My Documents\file.xls:STREAMNAME': file not found
03/22/2006 13:58:22 ANS1804E Selective Backup processing of
'\\cairo\c$\Program
Files\Tivoli\CDP_for_Files\TSMAuditFile-active.log_3_select_acp' finished
with failures.
```

Figure 3-50 Messages ANS1228E, ANS4005E, ANS1804E in the dsmerror.log

This is because the filelist TSMAuditFile-active.log_3_select_acp is passed to the TSM Backup/Archive command-line client containing two separate lines: one for the file itself (file.xls) and one for the file, including the stream name (file.xls:STREAMNAME).

Note: You can find the file TSMAuditFile-active.log_3_select_acp in the installation directory of Tivoli Continuous Data Protection for Files, which is, by default, C:\Program Files\Tivoli\CDP_for_Files (see 3.4.2, “IBM Tivoli Storage Manager specific log files” on page 111).

Figure 3-51 shows the content of the TSMAuditFile-active.log_3_select_acp file.

```
"C:\Documents and Settings\Administrator\My Documents\file.xls"
"C:\Documents and Settings\Administrator\My Documents\file.xls:STREAMNAME"
```

Figure 3-51 Content of the filelist TSMAuditFile-active.log_3_select_acp

The TSM Backup/Archive command-line client tries to back up each entry in the filelist, line by line. As the named stream STREAMNAME is hidden to the operating system, the TSM Backup/Archive command-line client fails to back up up file.xls:STREAMNAME, causing the error messages `ANS1228E Sending of object failed`, `ANS4005E File not found`, and `ANS1804E Selective Backup finished with failures` in the dsmerror.log file.

Figure 3-52 on page 102 shows the complete TSM Backup/Archive command-line client console output of this backup session, as seen in the file TSMout.log_acp.

Note: You can find the TSM Backup/Archive command-line client console output file TSMout.log_acp also in the installation directory of the Tivoli Continuous Data Protection for Files. For more information, refer to 3.4.2, “IBM Tivoli Storage Manager specific log files” on page 111.

```
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 3, Level 2.0
  Client date/time: 03/22/2006 13:58:21
(c) Copyright by IBM Corporation and other(s) 1990, 2005. All Rights Reserved.

Node Name: CAIRO_WS
Session established with server FLORENCE: Windows
  Server Version 5, Release 3, Level 2.0
  Server date/time: 03/22/2006 13:57:33  Last access: 03/22/2006 13:45:31

Selective Backup function invoked.

ANS1228E Sending of object '\\cairo\c$\Documents and Settings\Administrator\My
Documents\file.xls:STREAMNAME' failed
ANS4005E Error processing '\\cairo\c$\Documents and Settings\Administrator\My
Documents\file.xls:STREAMNAME': file not found
Directory-->                  0 \\cairo\c$\Documents and Settings [Sent]
Directory-->                  0 \\cairo\c$\Documents and Settings\Administrator [Sent]
Directory-->                  0 \\cairo\c$\Documents and Settings\Administrator\My
Documents [Sent]
Normal File-->        2,032,128 \\cairo\c$\Documents and Settings\Administrator\My
Documents\file.xls [Sent]
ANS1804E Selective Backup processing of '\\cairo\c$\Program
Files\Tivoli\CDP_for_Files\TSMAuditFile-active.log_3_select_acp' finished with failures.


Total number of objects inspected:       5
Total number of objects backed up:       4
Total number of objects updated:         0
Total number of objects rebound:         0
Total number of objects deleted:         0
Total number of objects expired:         0
Total number of objects failed:          1
Total number of subfile objects:         0
Total number of bytes transferred:     1.93 MB
Data transfer time:                    0.17 sec
Network data transfer rate:        11,546.89 KB/sec
Aggregate data transfer rate:        993.03 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:00:02
```

Figure 3-52 The TSM Backup/Archive command-line client console output with error messages

As you can see, the file file.xls itself is backed up successfully (`Normal File--> 2,032,128 \\cairo\c$\Documents and Settings\Administrator\My Documents\file.xls [Sent]`). However, sending file.xls:STREAMNAME failed (`ANS1228E`) as it was not found (`ANS4005E`).

Editing a file with named streams

When you edit and save the changes in an existing file with a named stream (we use file file.xls again in this example), this case is different compared to copying such a file.

In this case, the TSM Backup/Archive client error log file (dsmerror.log) shows the `ANS1345E No objects on server match...` messages (see Figure 3-53), while the console output of the TSM Backup/Archive command-line client session (TSMout.log_acp) looks fine.

```
03/22/2006 14:19:33 ANS1345E No objects on server match
'\\cairo\c$\Documents and Settings\Administrator\My
Documents\E9E31300:STREAMNAME'
03/22/2006 14:19:33 ANS1345E No objects on server match
'\\cairo\c$\Documents and Settings\Administrator\My Documents\E9E31300'
```

Figure 3-53 Error messages ANS1345E in the dsmerror.log

Figure 3-54 shows the console output of the TSM Backup/Archive command-line client session.

```
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 3, Level 2.0
  Client date/time: 03/22/2006 14:19:37
(c) Copyright by IBM Corporation and other(s) 1990, 2005. All Rights Reserved.

Node Name: CAIRO_WS
Session established with server FLORENCE: Windows
  Server Version 5, Release 3, Level 2.0
  Server date/time: 03/22/2006 14:18:49  Last access: 03/22/2006 14:18:45

Selective Backup function invoked.

Normal File-->         2,032,128 \\cairo\c$\Documents and Settings\Administrator\My
Documents\file.xls [Sent]
Selective Backup processing of '\\cairo\c$\Program
Files\Tivoli\CDP_for_Files\TSMAuditFile-active.log_3_select_acp' finished without failure.


Total number of objects inspected:        1
Total number of objects backed up:        1
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:     1.93 MB
Data transfer time:                    0.15 sec
Network data transfer rate:        12,643.70 KB/sec
Aggregate data transfer rate:         992.53 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:00:02
```

Figure 3-54 No error messages in the console output (TSMout.log_acp)

At this point, it is not clear where these error messages `ANS1345E No objects on server match...` come from and why they are not reported in TSMout.log_acp. The TSM server activity log may give here an additional hint. To view this log, you must be a registered administrator on the TSM server:

1. Select **Start** → **Run**, type **cmd**, and click **OK**. A Windows command-line window appears.

2. Change to the installation directory of the TSM Backup/Archive client by entering **cd "\program files\tivoli\tsm\baclient"**.
3. Start the TSM administrative command-line client by entering **dsmadmc**.

> **Attention:** By default, the TSM administrative command-line client (dsmadmc.exe) is not installed. If this is the case, refer to Chapter 1, "Installing Tivoli Storage Manager", in *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788 for details about how to install it.

4. When prompted, enter your administrative user identification (ID) name and password.
5. Type **query actlog** to display the TSM server activity log.

   A sample logon session to the TSM server using the TSM administrative command-line client is shown in Figure 3-55.

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\Program Files\Tivoli\TSM\baclient"

C:\Program Files\Tivoli\TSM\baclient>dsmadmc
IBM Tivoli Storage Manager
Command Line Administrative Interface - Version 5, Release 3, Level 2.0
(c) Copyright by IBM Corporation and other(s) 1990, 2005. All Rights Reserved.

Enter your user id:  admin

Enter your password:  *****

Session established with server FLORENCE: Windows
  Server Version 5, Release 3, Level 2.0
  Server date/time: 03/22/2006 19:41:44  Last access: 03/22/2006 19:12:32


tsm: FLORENCE>query actlog
```

Figure 3-55 Logging on to the TSM server using the TSM command-line client

In our example, two TSM Backup/Archive client sessions are opened on the TSM server for node name CAIRO_WS: session 1292 and session 1293.

Figure 3-56 shows session 1292.

```
03/22/2006 14:18:45   ANR0406I Session 1292 started for node CAIRO_WS (WinNT)
                       (Tcp/Ip cairo.xxx.yyy.zzz.com(1731)). (SESSION: 1292)
03/22/2006 14:18:48   ANE4952I (Session: 1292, Node: CAIRO_WS)  Total number
                       of objects inspected:        2 (SESSION: 1292)
03/22/2006 14:18:48   ANE4954I (Session: 1292, Node: CAIRO_WS)  Total number
                       of objects backed up:        0 (SESSION: 1292)
03/22/2006 14:18:48   ANE4958I (Session: 1292, Node: CAIRO_WS)  Total number
                       of objects updated:          0 (SESSION: 1292)
03/22/2006 14:18:48   ANE4960I (Session: 1292, Node: CAIRO_WS)  Total number
                       of objects rebound:          0 (SESSION: 1292)
03/22/2006 14:18:48   ANE4957I (Session: 1292, Node: CAIRO_WS)  Total number
                       of objects deleted:          0 (SESSION: 1292)
03/22/2006 14:18:48   ANE4970I (Session: 1292, Node: CAIRO_WS)  Total number
                       of objects expired:          0 (SESSION: 1292)
03/22/2006 14:18:48   ANE4959I (Session: 1292, Node: CAIRO_WS)  Total number
                       of objects failed:           2 (SESSION: 1292)
03/22/2006 14:18:48   ANE4961I (Session: 1292, Node: CAIRO_WS)  Total number
                       of bytes transferred:     0  B (SESSION: 1292)
03/22/2006 14:18:48   ANE4963I (Session: 1292, Node: CAIRO_WS)  Data transfer
                       time:                   0.00 sec (SESSION: 1292)
03/22/2006 14:18:48   ANE4966I (Session: 1292, Node: CAIRO_WS)  Network data
                       transfer rate:          0.00 KB/sec (SESSION: 1292)
03/22/2006 14:18:48   ANE4967I (Session: 1292, Node: CAIRO_WS)  Aggregate data
                       transfer rate:         0.00 KB/sec (SESSION: 1292)
03/22/2006 14:18:48   ANE4968I (Session: 1292, Node: CAIRO_WS)  Objects
                       compressed by:                    0% (SESSION: 1292)
03/22/2006 14:18:48   ANE4964I (Session: 1292, Node: CAIRO_WS)  Elapsed
                       processing time:          00:00:03 (SESSION: 1292)
03/22/2006 14:18:48   ANR0403I Session 1292 ended for node CAIRO_WS (WinNT).
                       (SESSION: 1292)
```

Figure 3-56 The TSM server activity log with session 1292 (expire session)

Figure 3-57 on page 107 shows session 1293.

```
03/22/2006 14:18:49   ANR0406I Session 1293 started for node CAIRO_WS (WinNT)
                       (Tcp/Ip cairo.xxx.yyy.zzz.com(1732)). (SESSION: 1293)
03/22/2006 14:18:51   ANE4952I (Session: 1293, Node: CAIRO_WS)  Total number
                       of objects inspected:        1 (SESSION: 1293)
03/22/2006 14:18:51   ANE4954I (Session: 1293, Node: CAIRO_WS)  Total number
                       of objects backed up:        1 (SESSION: 1293)
03/22/2006 14:18:51   ANE4958I (Session: 1293, Node: CAIRO_WS)  Total number
                       of objects updated:          0 (SESSION: 1293)
03/22/2006 14:18:51   ANE4960I (Session: 1293, Node: CAIRO_WS)  Total number
                       of objects rebound:          0 (SESSION: 1293)
03/22/2006 14:18:51   ANE4957I (Session: 1293, Node: CAIRO_WS)  Total number
                       of objects deleted:          0 (SESSION: 1293)
03/22/2006 14:18:51   ANE4970I (Session: 1293, Node: CAIRO_WS)  Total number
                       of objects expired:          0 (SESSION: 1293)
03/22/2006 14:18:51   ANE4959I (Session: 1293, Node: CAIRO_WS)  Total number
                       of objects failed:           0 (SESSION: 1293)
03/22/2006 14:18:51   ANE4965I (Session: 1293, Node: CAIRO_WS)  Elapsed
                       processing time (H:MM:SS): 0 (SESSION: 1293)
03/22/2006 14:18:51   ANE4961I (Session: 1293, Node: CAIRO_WS)  Total number
                       of bytes transferred:  1.93 MB (SESSION: 1293)
03/22/2006 14:18:51   ANE4963I (Session: 1293, Node: CAIRO_WS)  Data transfer
                       time:                    0.15 sec (SESSION: 1293)
03/22/2006 14:18:51   ANE4966I (Session: 1293, Node: CAIRO_WS)  Network data
                       transfer rate:       12,643.70 KB/sec (SESSION: 1293)
03/22/2006 14:18:51   ANE4967I (Session: 1293, Node: CAIRO_WS)  Aggregate data
                       transfer rate:       992.53 KB/sec (SESSION: 1293)
03/22/2006 14:18:51   ANE4968I (Session: 1293, Node: CAIRO_WS)  Objects
                       compressed by:                  0% (SESSION: 1293)
03/22/2006 14:18:51   ANE4969I (Session: 1293, Node: CAIRO_WS)  Total
                       failures:                        0 (SESSION: 1293)
03/22/2006 14:18:51   ANE4964I (Session: 1293, Node: CAIRO_WS)  Elapsed
                       processing time:           00:00:02 (SESSION: 1293)
03/22/2006 14:18:51   ANR0403I Session 1293 ended for node CAIRO_WS (WinNT).
                       (SESSION: 1293)
```

Figure 3-57 The TSM server activity log with session 1293 (backup session)

Due to the way in which Windows works when you open, edit, save, and close a file, a temporary instance of the file is created and immediately deleted. This is tracked by the Tivoli Continuous Data Protection for Files and stored in file TSMAuditFile-active.log_4_expire_acp.

Note: You can find the file TSMAuditFile-active.log_4_expire_acp in the installation directory of the Tivoli Continuous Data Protection for Files (C:\Program Files\Tivoli\CDP_for_Files by default). For more details, refer to Section 3.4.2, “IBM Tivoli Storage Manager specific log files” on page 52.

Figure 3-58 shows the content of TSMAuditFile-active.log_4_expire_acp. This file is passed to the TSM Backup/Archive client as a list of files to expire on the TSM server, which can be seen as session 1292 for node name CAIRO_WS in the TSM server activity log (see Figure 3-56 on page 106).

```
"C:\Documents and Settings\Administrator\My Documents\E9E31300:STREAMNAME"
"C:\Documents and Settings\Administrator\My Documents\E9E31300"
```

Figure 3-58 Files to expire on the Tivoli Storage Manager server (TSMAuditFile-active.log_4_expire_acp)

As these files have never been stored on the TSM server, the messages `ANS1345E No objects on server match...` appear in the dsmerror.log (see Figure 3-53 on page 103). Because we have made changes to file file.xls, the file has to be backed up again. Figure 3-59 shows the content of file TSMAuditFile-active.log_3_select_acp, which keeps track of this and which is handed over to the TSM Backup/Archive client as the input list for files to back up.

```
"C:\Documents and Settings\Administrator\My Documents\file.xls"
```

Figure 3-59 TSMAuditFile-active.log_3_select_acp

The TSM Backup/Archive client backup session can be seen in the TSM server activity log as session 1293 (see Figure 3-57 on page 107). As this backup session starts *after* the expiration session (1292) and because it is successful, the console output of the TSM Backup/Archive command-line client session TSMout.log_acp (see Figure 3-54 on page 104) does not show any errors.

Summary

There are several issues with files containing named streams leading to different kinds of error messages in the TSM Backup/Archive client error log file (dsmerror.log). It is not possible to prevent them from appearing in the dsmerror.log; therefore, whenever you see an error message relating to a named stream, you know where it comes from and why it is issued.

3.4 Log files and FPcommand.bat

The following section provides some information about the log files created and used by Tivoli Continuous Data Protection for Files. The in-depth knowledge about those log files and their structure will not be handled here, as this is not necessary for the daily use of Tivoli Continuous Data Protection for Files.

Anyhow, they might be of interest for IBM support personnel for deeper problem determination in case you need to report a problem to them.

The Tivoli Continuous Data Protection for Files logs are created, transparently to the user, in the installation directory of Tivoli Continuous Data Protection for Files (C:\Program Files\Tivoli\CDP_for_Files by default).

Note: You *might not* find all of the mentioned logs in your Tivoli Continuous Data Protection for Files installation directory, as some of the log files are only used temporarily while others depend on how you have configured Tivoli Continuous Data Protection for Files.

3.4.1 Tivoli Continuous Data Protection for Files logs

Tivoli Continuous Data Protection for Files uses various logs for reporting or tracking its activities. Those log files are explained in this section of the chapter.

Installation log files

In Table 3-3, you can see the log files created during installation of Tivoli Continuous Data Protection for Files. They are helpful in case you have trouble getting Tivoli Continuous Data Protection for Files installed on your system.

Table 3-3 Installation log files

Log file name	Description
log.txt	This is the InstallShield log file.
fpinstall.log	The file fpinstall.log contains the installation information fromTivoli Continuous Data Protection for Files itself.
install.txt	File install.txt is a by-product of InstallShield. It is created to force InstallShield to reboot if it is an over-installation.

Replication logs

The log files regarding the replication activities of Tivoli Continuous Data Protection for Files are explained in Table 3-4.

Table 3-4 Replication logs

Log file name	Description
replication.log	The log file replication.log contains the last replication transactions (limited in size to 1.3 MB).
replication-queued.N (where N=0...9)	Queued replication transactions are written into file replication-queued.N.
replication-active.N (where N=0...9)	File replication-active.N contains the currently active replication transactions.
replication-failed.N (where N=0...9)	Failed replication transactions are reported in log file replication-failed.N (not limited in size).

Scheduled protection logs

Table 3-5 summarizes the various log files used when scheduled protection has been enabled in the configuration menu of the Tivoli Continuous Data Protection for Files Graphical User Interface (GUI).

Table 3-5 Scheduled protection logs

Log file name	Description
ChangeJournal.log	The file ChangeJournal.log does contain a list of all files pending for scheduled processing.
ChangeJournal.log_1_inprocess	Currently processed files are reported in file ChangeJournal.log_1_inprocess.
ChangeJournal.log_2_last	File ChangeJournal.log_2_last is containing the last files being processed.
ChangeJournal.log_3_out	ChangeJournal.log_3_out is empty.
ChangeJournal.log_LastSuccess	File ChangeJournal.log_LastSuccess contains the date and time of the last successful scheduled backup (as seen in the summary section for scheduled protection in the Tivoli Continuous Data Protection for Files GUI).

Log file name	Description
RemoteVersions.log	File RemoteVersions.lo holds an entry for each “versioned” file stored at the remote target.
purge_struggled.log	Files that appear unreachable during purge are reported in file purge_struggled.log.

Local pool log file and gendb

The local pool log file and the directory gendb are explained in Table 3-6.

Table 3-6 Local pool log file and gendb

Log file name	Description
LocalPool.log	The file LocalPool.log is a list of all files currently being in the local file pool (backup area).
gendb (directory)	The directory gendb and its subdirectories respectively hold version names with dates to facilitate pruning based on the retention settings.

3.4.2 IBM Tivoli Storage Manager specific log files

Depending on whether you are using IBM Tivoli Storage Manager (TSM) for either continuous data protection of your most important files or for scheduled protection of your regular files (or both combined), Tivoli Continuous Data Protection for Files creates and uses different log files for tracking the work to be done or reporting what activities have already been taken.

Using IBM Tivoli Storage Manager for continuous protection

Table 3-7 shows the Tivoli Continuous Data Protection for Files logs when you are using IBM Tivoli Storage Manager (TSM) for continuous data protection of your most important files.

Table 3-7 Log files when IBM Tivoli Storage Manager is used for continuous protection

Log file name	Description
TSMAuditFile-queue.log	File TSMAuditFile-queue.log contains an accumulating list of current files that need to be processed at the next TSM backup/expiration cycle.
TSMAuditFile-active.log	TSMAuditFile-active.log is a temporary file containing the current list of files in the process of being sent to the TSM server.
TSMAuditFile-active.log_2_pack	File TSMAuditFile-active.log_2_pack contains the list of files after duplicates have been removed.
TSMAuditFile-active.log_3_select	See TSMAuditFile-active.log_3_select_acp.
TSMAuditFile-active.log_3_select_acp	File TSMAuditFile-active.log_3_select_acp is the list of files being passed over to the TSM Backup/Archive command-line client for selective backup processing. This is the input file for the TSM Backup/Archive command-line client option -filelist.
TSMAuditFile-active.log_4_expire	See TSMAuditFile-active.log_4_expire_acp.
TSMAuditFile-active.log_4_expire_acp	File TSMAuditFile-active.log_4_expire_acp contains the list of files to expire on the TSM server. For expiration precessing, it is handed over to the TSM Backup/Archive command-line client as an argument for option -filelist.
TSMout.log	See TSMout.log_acp.
TSMout.log_acp	TSMout.log_acp is the re-directed output file of the last TSM Backup/Archive command-line client session (either expiration or selective backup)

Using IBM Tivoli Storage Manager for scheduled protection

If you are using IBM Tivoli Storage Manager (TSM) for scheduled protection of your regular files, you can see in Table 3-8 what log files are used in this case by Tivoli Continuous Data Protection for Files.

Table 3-8 Log files when IBM Tivoli Storage Manager is used for the scheduled protection

Log file name	Description
sysprotect_tsm_select_acp	For selective backup processing, the file sysprotect_tsm_select_acp contains the list of files to be processed by the TSM Backup/Archive command client. This file is passed to the TSM Backup/Archive command-line client as the input file for the -filelist command-line option.
sysprotect_tsm_select_out	See sysprotect_tsm_select_out_acp.
sysprotect_tsm_select_out_acp	File sysprotect_tsm_select_out_acp is the re-directed output file of the selective backup session of the TSM Backup/Archive command-line client.
sysprotect_tsm_expire_acp	The file sysprotect_tsm_expire_acp is the list of files to expire on the TSM server. For expiration precessing, it is handed over to the TSM Backup/Archive command-line client as an argument for option -filelist.
sysprotect_tsm_expire_out	See sysprotect_tsm_expire_out_acp.
sysprotect_tsm_expire_out_acp	File sysprotect_tsm_expire_out_acp contains the console output of the TSM Backup/Archive command-line client session for expiring files on the TSM server.

3.4.3 File FPcommand.bat

Tivoli Continuous Data Protection for Files starts the TSM Backup/Archive command-line client (dsmc.exe) indirectly. It does so by creating and executing a Windows batch file named FPcommand.bat.

Attention: Unlike the logs of Tivoli Continuous Data Protection for Files, the file FPcommand.bat *cannot* be found in the Tivoli Continuous Data Protection for Files installation directory but in the installation directory of the TSM Backup/Archive client (by default, C:\Program Files\Tivoli\TSM\baclient).

The FPcommand.bat file will be newly created - or overwritten, if it already exists - each time the TSM Backup/Archive client is invoked by Tivoli Continuous Data Protection for Files. Depending if files need to be backed up (continuously or scheduled) or files need to expire on the TSM server (continuously or scheduled), the FPcommand.bat has different content.

Using IBM Tivoli Storage Manager for continuous protection

When you are using IBM Tivoli Storage Manager (TSM) for continuos data protection of your very important files, the file FPcommand.bat looks like as seen in Figure 3-60 (selective backup) or Figure 3-61 (expiration).

```
set DSM_CDP=1
cd /d "C:\Program Files\Tivoli\TSM\baclient"
"C:\Program Files\Tivoli\TSM\baclient\dsmc" sel -filelist="C:\Program
Files\Tivoli\CDP_for_Files\TSMAuditFile-active.log_3_select_acp"
>>"C:\Program Files\Tivoli\CDP_for_Files\TSMout.log_acp"
```

Figure 3-60 FPcommand.bat when using TSM for continuous data protection

```
set DSM_CDP=1
cd /d "C:\Program Files\Tivoli\TSM\baclient"
"C:\Program Files\Tivoli\TSM\baclient\dsmc" expire -noprompt
-filelist="C:\Program
Files\Tivoli\CDP_for_Files\TSMAuditFile-active.log_4_expire_acp"
>>"C:\Program Files\Tivoli\CDP_for_Files\TSMout.log_acp"
```

Figure 3-61 FPcommand.bat when using TSM for continuous data protection

Using IBM Tivoli Storage Manager for scheduled protection

Figure 3-62 (selective backup) and Figure 3-63 on page 115 (expiration) shows the file FPcommand.bat in case you are using IBM Tivoli Storage Manager (TSM) for scheduled data protection.

```
set DSM_CDP=1
cd /d "C:\Program Files\Tivoli\TSM\baclient"
"C:\Program Files\Tivoli\TSM\baclient\dsmc" sel -filelist="C:\Program
Files\Tivoli\CDP_for_Files\sysprotect_tsm_select_acp" >>"C:\Program
Files\Tivoli\CDP_for_Files\sysprotect_tsm_select_out_acp"
```

Figure 3-62 FPcommand.bat when using TSM for scheduled data protection

```
set DSM_CDP=1
cd /d "C:\Program Files\Tivoli\TSM\baclient"
"C:\Program Files\Tivoli\TSM\baclient\dsmc" expire -noprompt
-filelist="C:\Program Files\Tivoli\CDP_for_Files\sysprotect_tsm_expire_acp"
>>"C:\Program Files\Tivoli\CDP_for_Files\sysprotect_tsm_expire_out_acp"
```

Figure 3-63 FPcommand.bat when using TSM for scheduled data protection

3.5 Tracing

For problem determination, Tivoli Continuous Data Protection for Files has a built-in tracing functionality. In this section, we will show you the basics of how to capture a Tivoli Continuous Data Protection for Files trace as well as a short tracing example.

Important: Tracing facilities are used by Tivoli Continuous Data Protection for Files product development and IBM support personnel for diagnosing and debugging problems and *should only be used when requested* by them. These facilities are subject to change without notice and may vary depending upon the version and release of the product.

Before you start

In order to view the Tivoli Continuous Data Protection for Files trace output, you need to have DebugView installed. DebugView is a program to display both Win32® and kernel-mode debug output. It can be downloaded from the Sysinternals Web site:

http://www.sysinternals.com/utilities/debugview.html

For installation instructions and usage of DebugView, please refer to the same URL.

How to run a trace

Tracing will be started using the FilePath agent (fpa) executable fpa.exe found in the installation directory of Tivoli Continuous Data Protection for Files. The FilePath agent is a configuration/reporting tool as well as a daemon. It can be run with command-line parameters (as commands) that will get processed and then exits/returns or in an interactive mode where it awaits user-typed commands and responds after each one. In our example (see “Tracing example” on page 117), we will use the FilePath agent interactively.

Note: Please have a look at Chapter 2, “Product architecture, planning, and deployment” on page 17 to get more information about the FilePath agent (fpa.exe).

Trace syntax:

```
trace [level=FINE/MEDIUM/COARSE] [device=FILE/SCREEN] [program=programname]
mask=BASIC,ALL,SYS,HOOK,HOOK_IO,FPA,REPLQ,REPLT,REPLK,REPLD,LOG,EXEC,AUDIT,FPL,
FPL_OPEN,FPL_WRITE,FPL_CLOSE,FPL_LIST,FPL_META,HTML,HTML_SET,HTML_GET,HTML_REST
ORE,DEBUG1,XML,FPQ,METRIC,ERR,HASH,IOCTL,PF,FILE,LRP,ANALFS,ANALFS_XML,ANALFS_F
ILES,EXPUNGE,FNAME,WORM,CAS,TABULATION,MIRROR_META,MIRROR_IO,MIRROR_IOLIST,MIRR
OR_SIZE,MIRROR_DRAINER
```

Parameters:

- level

  Specifies the granularity of trace messages being reported.

  - FINE

    Specifies that all messages are logged.

    Attention: This may create a huge amount of output depending on the trace mask(s) being used.

  - MEDIUM

    Specifies that the most important messages are logged.

  - COARSE

    Specifies that only a few messages are logged.

- device

  Specifies the system logging target.

  - FILE

    Specifies the system error log file as the logging target.

    Attention: The system error log (file) of Windows operating systems is the Windows event log. Using device=FILE on Windows is *not recommended*, as the trace output would be written into the Windows system event log and flood it with (lots of) error messages.

- SCREEN

  Specifies the current terminal device of the active process as the logging target.

- program

  Specifies to filter a particular program's interaction.

  - programname

    Specifies the name of the particular program to monitor.

- mask

  Specifies the trace mask(s). In case multiple trace masks are used, this is a comma separated list of trace masks.

Tracing example

The following section demonstrates how to capture a Tivoli Continuous Data Protection for Files trace. The trace mask we are using (`mask=fpl_meta`) in this example is to show how Tivoli Continuous Data Protection for Files iterates through the exclude and include list to check if a file needs to be processed or not.

Important: Before activating the Tivoli Continuous Data Protection for Files trace, you need to execute the DebugView program by double-clicking the DebugView program file (dbgview.exe). DebugView will immediately start capturing debug output.

Use the following steps to start the FilePath agent (see also Figure 3-64 on page 118):

1. Select **Start** → **Run**, type **cmd**, and press **OK**. A Windows command-line window appears.
2. Change to the installation directory of Tivoli Continuous Data Protection for Files by entering **cd "\program files\tivoli\cdp_for_files"**.
3. To run the FilePath agent in interactive mode, enter **fpa**.

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\program
files\tivoli\cdp_for_files"

C:\Program Files\Tivoli\CDP_for_Files>fpa
fpa>
```

Figure 3-64 FilePath agent in interactive mode

The `fpa>` command prompt indicates that you are now using the FilePath agent interactively. Enter, on the `fpa>` command prompt, the **`trace`** command, as seen in Figure 3-65, to start the trace:

```
fpa>trace level=fine device=screen program=cmd.exe mask=fpl_meta
```

Figure 3-65 Command to start a Tivoli Continuous Data Protection for Files trace

By specifying the **`trace`** command parameter program=cmd.exe, we are filtering the trace for Windows command-line (cmd.exe) activities only. This helps us reducing the information being captured in the trace though we are using the finest trace granularity (level=fine).

Select **Start** → **Run**, type **`cmd`**, and press **OK** to open a second Windows command-line window. To trigger an activity, create a file that is defined in your Tivoli Continuous Data Protection for Files configuration as a file for continuous data protection (see Figure 3-27 on page 79), for example, by running **`echo test >> c:\file.doc`**, as shown in Figure 3-66.

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>echo test >> c:\file.doc

C:\Documents and Settings\Administrator>
```

Figure 3-66 Create file.doc to trigger an activity

Immediately after you have issued the command, the DebugView program is capturing the trace (debug) output, as you can see in Figure 3-67 on page 119.

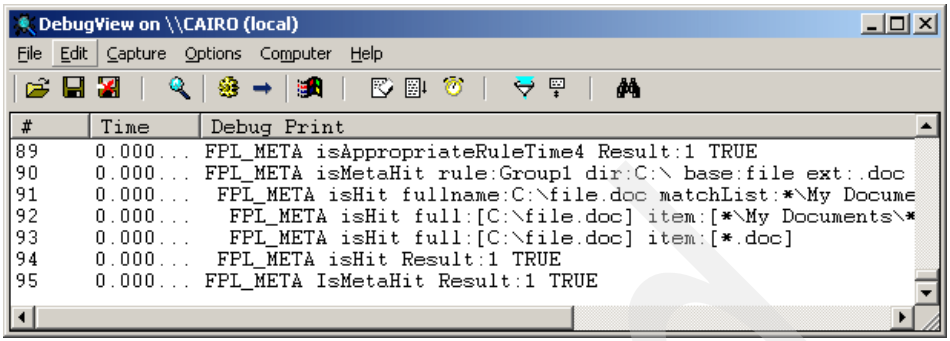


Figure 3-67 DebugView capturing the trace output

To end tracing, enter a **trace** command with an empty trace mask (see Figure 3-68).

```
fpa>trace mask=""
```

Figure 3-68 Command to stop the trace

By entering **quit** or **exit** on the fpa> command prompt, you can leave the FilePath agent again (see Figure 3-69).

```
fpa>quit

C:\Program Files\Tivoli\CDP_for_Files>
```

Figure 3-69 Quitting the interactive mode of the FilePath agent

Example 3-1 on page 120 shows an excerpt from the complete trace tripped by creating the file named file.doc. You can see that the complete file name (C:\file.doc) gets decomposed into its components: the directory (C:\), the base (file), and the extension (.doc). Afterwards, the file name is first matched against the exclude and then against the include list. As we defined files with extension “doc” for continuous data protection, the latter one is a hit (IsMetaHit Result:1 TRUE), and the action gets executed: file.doc is processed for continuous data protection.

Example 3-1 Tracing example (trace mask=fpl_meta)

```
000000620.00062047FPL_META IsMetaHit Result:0 FALSE
000000630.00062888FPL_META isAppropriateRuleTime rule:Group0 writable:1 meta.when OpenRW
isDir:0 meta.select:Dirs&Files
000000640.00063444FPL_META isAppropriateRuleTime4 Result:1 TRUE
000000650.00064375FPL_META isMetaHit rule:Group0 dir:C:\ base:file ext:.doc
000000660.00066157 FPL_META isHit fullname:C:\file.doc matchList:RealTimeBackup|\Program
Files|~|C:\WINDOWS\system32|*.tmp|*.temp|\Temp\|\Temporary|\Windows|\System
Volume|\tsmlvsacache|\cache match:Contains
000000670.00067276  FPL_META isHit full:[C:\file.doc] item:[RealTimeBackup]
000000680.00068317  FPL_META isHit full:[C:\file.doc] item:[\Program Files]
000000690.00069306  FPL_META isHit full:[C:\file.doc] item:[~]
000000700.00070557  FPL_META isHit full:[C:\file.doc] item:[C:\WINDOWS\system32]
000000710.00071613  FPL_META isHit full:[C:\file.doc] item:[*.tmp]
000000720.00072648  FPL_META isHit full:[C:\file.doc] item:[*.temp]
000000730.00073654  FPL_META isHit full:[C:\file.doc] item:[\Temp\]
000000740.00074668  FPL_META isHit full:[C:\file.doc] item:[\Temporary]
000000750.00075671  FPL_META isHit full:[C:\file.doc] item:[\Windows]
000000760.00076689  FPL_META isHit full:[C:\file.doc] item:[\System Volume]
000000770.00077707  FPL_META isHit full:[C:\file.doc] item:[\tsmlvsacache]
000000780.00078696  FPL_META isHit full:[C:\file.doc] item:[\cache]
000000790.00079307 FPL_META isHit Result:0 FALSE
000000800.00079810FPL_META IsMetaHit Result:0 FALSE
000000810.00080673FPL_META isAppropriateRuleTime rule:ChangeJournal writable:1 meta.when OpenRW
isDir:0 meta.select:Dirs&Files
000000820.00081227FPL_META isAppropriateRuleTime4 Result:1 TRUE
000000830.00082186FPL_META isMetaHit rule:ChangeJournal dir:C:\ base:file ext:.doc
000000840.00083216 FPL_META isHit fullname:C:\file.doc matchList:doesntmatter match:Contains
000000850.00084269  FPL_META isHit full:[C:\file.doc] item:[doesntmatter]
000000860.00084880 FPL_META isHit Result:0 FALSE
000000870.00085382FPL_META IsMetaHit Result:0 FALSE
000000880.00087788FPL_META isAppropriateRuleTime rule:Group1 writable:1 meta.when OpenRW
isDir:0 meta.select:Dirs&Files
000000890.00088343FPL_META isAppropriateRuleTime4 Result:1 TRUE
000000900.00089276FPL_META isMetaHit rule:Group1 dir:C:\ base:file ext:.doc
000000910.00090440 FPL_META isHit fullname:C:\file.doc matchList:*\My
Documents\*|*.doc|*.xls|*.ppt|*.123 match:Contains
000000920.00091557  FPL_META isHit full:[C:\file.doc] item:[*\My Documents\*]
000000930.00092586  FPL_META isHit full:[C:\file.doc] item:[*.doc]
000000940.00093217 FPL_META isHit Result:1 TRUE
000000950.00093720FPL_META IsMetaHit Result:1 TRUE
```

4

Use case scenarios

This chapter will describe some typical use cases where Tivoli Continuous Data Protection for Files can be deployed in various configurations and settings. In some cases, only Tivoli Continuous Data Protection for Files is deployed, and in some, it is integrated with the use of TSM.

The following use cases are described in this chapter:

- Using Tivoli Continuous Data Protection for Files in a single-user environment
- Multiple computers in a home or small business
- Multiple users in a large enterprise environment
- Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager working together

4.1 Using Tivoli Continuous Data Protection for Files in a single-user environment

Because Tivoli Continuous Data Protection for Files is a highly flexible product, it can be scaled to be useful both in a large corporate environment as well as on a single computer that is used either for work or at home. Two likely scenarios will be discussed here:

- Single computer with no network connection
- Single computer with an ISP connection to external storage

4.1.1 Single computer with no network connection

Even though it seems like most computers are connected to a network of some sort, there are still users who have a single computer and who store all of their information on the computer's hard drive. This computer could either be a desktop or mobile computer. Two use cases fall under this description:

1. Stand alone with no external storage.
2. Stand alone with removable storage device (USB or firewire drive)

Stand alone with no external storage

Even without access to a network with remote storage capability, Tivoli Continuous Data Protection for Files can be configured to provide a high level of protection.

In this case, the recommended settings would be:

- Local Continuous backup: Enabled, 2 GB pool, Include MS Office file extensions and other user-created content that is considered high value.
- Remote Continuous backup: Disabled. No network.
- TSM Continuous backup: Disabled. No TSM.
- Scheduled backup: Disabled. No network.

In this scenario, the local pool of versioned back up files provides the highest level of protection on a stand alone computer. One important consideration in this configuration is the File List for files included in Continuous replication. In the case where there is a remote backup location, the Scheduled backup provides a safety net to catch files on the computer that are not caught by the Local Continuous backup File List. So, it may be advisable to perform the fine tuning exercises (see "Fine tuning" on page 41 for more information) fairly frequently after the initial installation to make sure all of the important files are being saved (and non-essential files are excluded).

Stand alone with removable storage device

This scenario is similar to the case above, with the addition of some sort of external, removable hard drive. This could be a USB device that connects through a USB port, or a device that connects through a firewire port. In this scenario, the external drive is not always connected to the computer; most likely, this would be the case with a mobile computer that moves around.

For this case, the recommended settings are:

- Local Continuous backup: Enabled, 2 GB pool, Include MS Office file extensions and other user-created content that is considered high value.
- Remote Continuous backup: Disabled. In this case, since you will only be attaching the storage device periodically, this option would be unnecessary.
- TSM Continuous backup: Disabled. No TSM.
- Scheduled backup: Enabled, Daily or Weekly. 10 GB pool (or approximately a sixth to a tenth the size of the source disks), Versions optional. Broader inclusion list than local, or consider "*" as the File List.

> **Note:** When you configure your removable storage device, make sure that you select it from the Remote location Browse list. There is currently a bug in the software that allows some removable devices to show up in the Local backup list. You should not select the removable device from the Local pick list.

In this case, there are a few options that depend on how large your external storage device is, and how often you plan to connect and backup to it. If you are working on critical files and make numerous changes every day, you might want to set the backup period to daily and make sure that you have a large pool, with five versions. This requires significant space on the external drive, but it does provide a very high level of protection.

If you are confident that your local backup is generally sufficient, you may want to set the remote backup schedule to weekly and reduce the versions to 0. This will still provide an extra layer of protection, without requiring either a large external storage device, or that it be connected every day. In either case, if you are not connected when the scheduled time is due, Tivoli Continuous Data Protection for Files will keep the list of files to be backed up and wait until you are connected.

4.1.2 Single computer with an ISP connection

This scenario represents a user who has a single computer, either mobile computer or desktop, that has access to external storage through an ISP. For this user, all files are saved on the local machine, and the remote storage on the ISP's server is used primarily for occasional backups. The local backup repository still provides the primary method of protection, but the remote backup location is important for providing off-site storage.

In this scenario, the recommended configuration is:

- Local Continuous backup: Enabled, 2 GB pool, Include MS Office file extensions and other user-created content that is considered high value.
- Remote Continuous backup: Disabled. It is unnecessary to add this load on the Internet traffic, and the ISP storage site.
- TSM Continuous backup: Disabled. No TSM.
- Scheduled backup: Enabled, Daily. 10 GB pool (or approximately a sixth to a tenth the size of the source disks), five versions, broader inclusion list than local. Alternatively, set the inclusion to "*" and schedule a weekly backup.

If the storage space you have available on your ISP is limited, you may want to narrow the inclusion list for the Scheduled backup to save space. Alternatively, you could set the versions to 0.

4.2 Multiple computers in a home or small business

In this scenario, there are multiple computers connected to a single network with a file server. This could be in a home or in a small business. The setup includes ample storage space connected to a network file server. This could either be a single computer with a large internal hard drive, or an older computer with an external hard drive attached to it. This latter case is shown in Figure 4-1 on page 125, but it could also represent a small business configuration.

Each computer will have Tivoli Continuous Data Protection for Files installed locally and configured for each user's needs. In general, the recommended configuration is:

- Local Continuous backup: Enabled, 2 GB pool, Include user-created content that is considered high value.
- Remote Continuous backup: Disabled. It is unnecessary to add this load to the network traffic.
- TSM Continuous backup: Disabled. No TSM.

- Scheduled backup: Enabled, Daily for mobile computers that are disconnected from the network at different intervals, weekly for desktops that are consistently in the network. 10 GB pool (or approximately a sixth to a tenth the size of the source disks), five versions, broader inclusion list than local. Alternatively, set the inclusion to “*” and schedule a weekly backup.

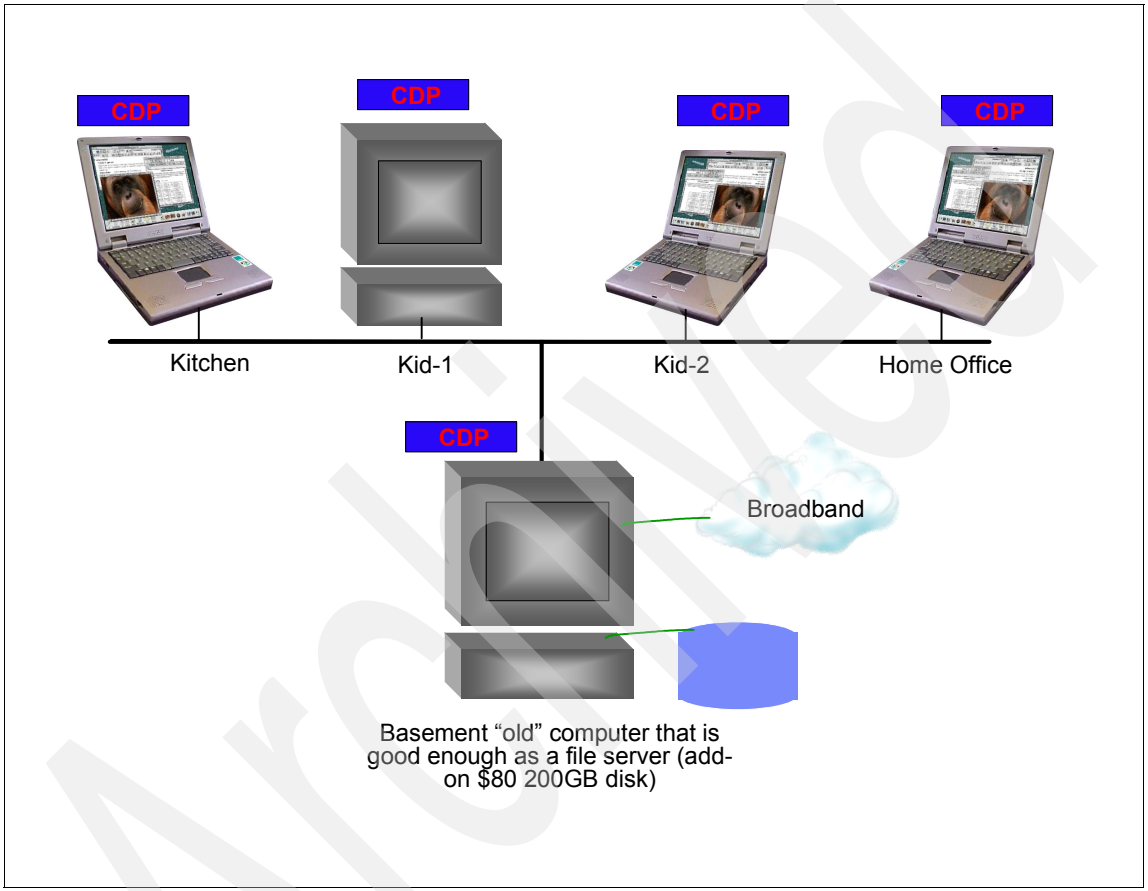


Figure 4-1 Home or small office configuration

In this configuration, it is important to make sure that each computer has a File List that includes the file types and directories used most by the particular user. For example, home users might have files from digital cameras, music files, or other proprietary file formats that could be stored outside of the \My Documents\ directory structure. Each computer is configured to back up to the remote file server.

If you want to have extra security on the backup server, you can also install Tivoli Continuous Data Protection for Files on the server and set up the Vault function. You can disable both local and remote replication and go directly to the Vault window. In the File List for the Vault function, add in the top folder for each computer that is currently backing up to the server if you want to lock down all of the files. Alternatively, you could only add in particular file types or directories, for example, your digital pictures or mp3 files, if you want to limit the extra protection from deletion and alteration to certain files.

Tip: If you are going to invoke the Vault feature on a backup location, you will have to remove the \RealTimeBackup\ folder from the default Exclusion list. Otherwise, none of your files will be included in the Vault function.

4.3 Multiple users in a large enterprise environment

If you are going to deploy Tivoli Continuous Data Protection for Files in a large environment (without TSM), we recommend that an administrator sets up and deploys the installations. In the simplest case, Tivoli Continuous Data Protection for Files can be installed on a file server and configured to send protected files to a backup file server. In a more complex environment, especially one where mobile computers are used and systems are often off the network, Tivoli Continuous Data Protection for Files can additionally be deployed to each user's computer. With the use of push installation and automatic upgrades, it is relatively easy to deploy Tivoli Continuous Data Protection for Files to a large number of computers.

4.3.1 Tivoli Continuous Data Protection for Files on a file server

In this scenario, all computers in the network are already saving their files to a network location. The use of local files is minimal and the network file server is the primary work file location. See Figure 4-2 on page 127 for a diagram of this setup. The administrator only has to install Tivoli Continuous Data Protection for Files on the file server and set it up so that it is backing up all directories that contain user's data.

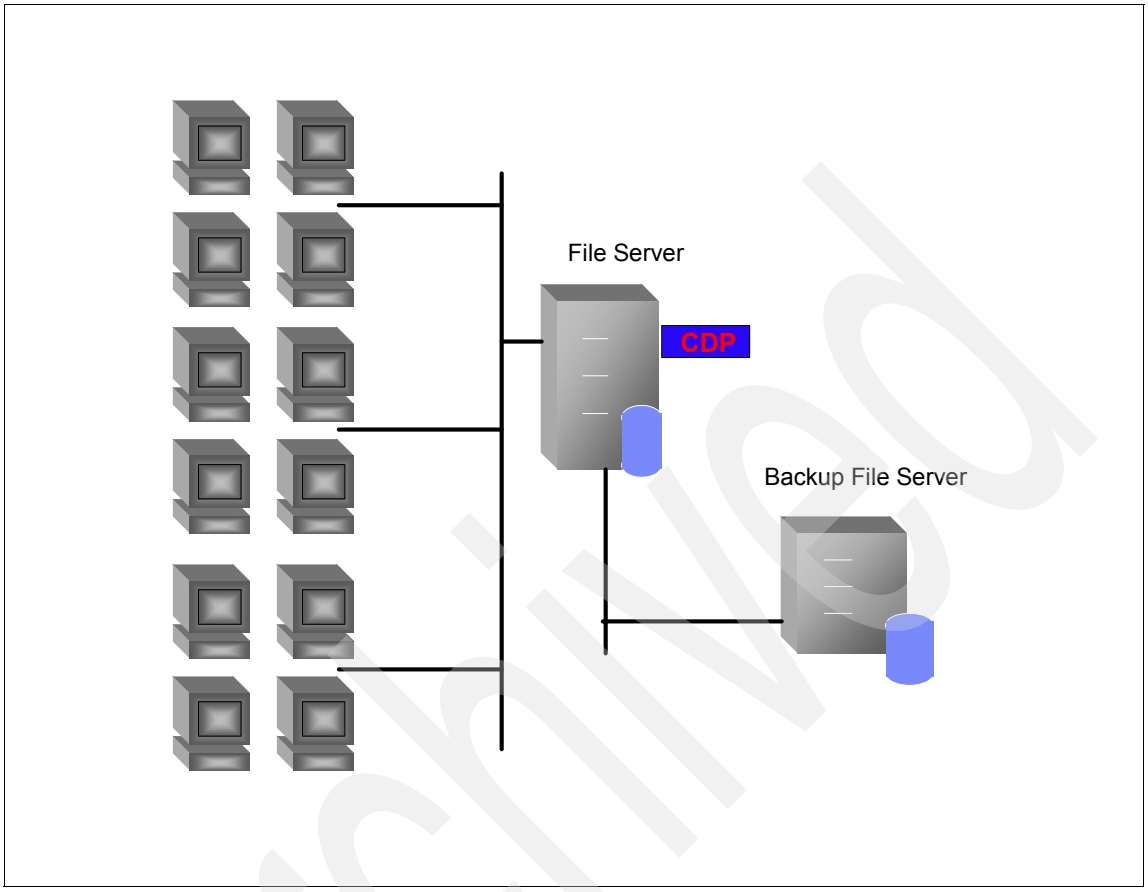


Figure 4-2 Simple deployment of Tivoli Continuous Data Protection for Files in a large environment

In this scenario, the recommended configuration is:

- Local Continuous backup: Disabled, files are protected on the remote server.
- Remote Continuous backup: Enabled (Optional). If this is the only backup utility for the file server, this would be desired. Include all users' directories.
- TSM Continuous backup: Disabled. No TSM.
- Scheduled backup: Enabled (Optional), Daily. Pool should be approximately five times the space allocated to all users, five versions, include all users' directories.

You may want to configure the product differently, depending on how much storage space you have on each server. We recommend that you use either the Continuous or Scheduled backup to the backup file server, depending on how current you need the backups to be. You could set the Scheduled backup to hourly if you prefer; however, Continuous backup would spread out the traffic over the network to the backup file server more evenly.

4.3.2 Distributed installation of Tivoli Continuous Data Protection for Files

If you are in an environment with a large number of computers, possibly both desktops and mobile computers, then you should consider using centralized configuration and deployment. Although it does not take a lot of time to install and configure Tivoli Continuous Data Protection for Files, if you need to deploy the product to a large number of computers, this could add up to a significant amount of time. Also, by centrally administering the deployment, you can set up corporate-wide configurations and ensure that all computers are being protected in the same manner. Thus, once the administrator has found out which are truly the highest value files, the configuration can be tailored either to the whole environment or by user profiles. See Figure 4-3 on page 129 for a diagram of this deployment.

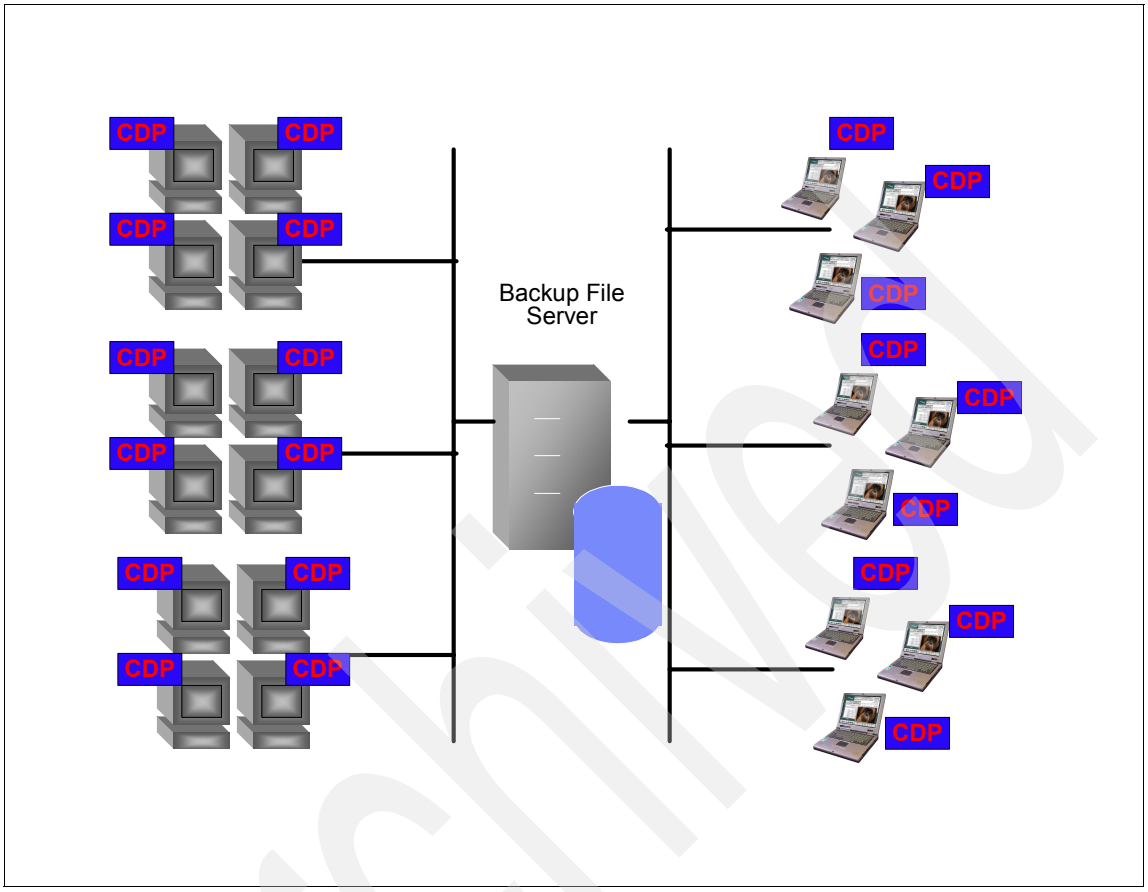


Figure 4-3 Distributed deployment of Tivoli Continuous Data Protection for Files in a large environment

To deploy Tivoli Continuous Data Protection for Files in this type of an environment, there are several steps involved in preparation, installation, and maintenance:

1. Install Tivoli Continuous Data Protection for Files on a single machine (master computer), which represents a typical configuration in the work environment.
2. Configure Tivoli Continuous Data Protection for Files, based on general considerations described in 2.2, “Planning for deployment” on page 26 and 2.3, “Deployment” on page 29.
3. Use the computer in a typical fashion and perform the fine tuning activity described in “Fine tuning” on page 41.

4. Once you are satisfied that the Tivoli Continuous Data Protection for Files configuration is optimized for your environment, open the user interface and go to the Reports window. Click the **Publish** button. This will create a file called “fpcommands.xml” in the global download directory, for example:

   \\MyServer\MyShare\RealTimeBackup\BackupAdmin\Downloads\fpcommands.xml

5. Copy this file to your local system, rename it to fpa.txt, and package it with our push installer program (or another commercially available software distribution tool).
6. Either run the push install to each target computer, or create a batch file to install to all computers at once.
7. Once the installations are complete, check the network backup location to verify that each computer has a directory under the top-level \RealTimeBackup\ folder.
8. If you need to make changes to the configuration, make them on the master computer and click the **Publish** button again. This new configuration will be automatically recognized and updated on all remote installations.
9. When there is a patch or upgrade installation of the product, copy the installer to the \BackupAdmin\Downloads directory (see Step 4. above). All remote installations will detect this; download the installer and install it automatically.

These steps describe deploying a single configuration to all computers. It is also possible to have several different configurations if you have several different profiles you need to take into consideration. You can distribute different configurations from the same file server, but each configuration will have to come from a different top-level share on the backup server. For example, you might have:

- \\MyServer\Sales\ for Sales people with mobile computers that are frequently on the road
- \\MyServer\Admins\ for office administrators with desktops
- \\MyServer\HR\ for specific applications on desktops

Each share can have a specific configuration that is tailored to the applications being used by each group, their general accessibility to the network, and other considerations.

Note: These instructions are intentionally general and do not provide exact details on how to package the installer. For detailed information on this topic, consult IBM Support or review the Tech Notes provided on the support Web site:

http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliContinuousDataProtectionforFiles.html

4.4 Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager working together

In this section, we show you a possible scenario of how Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager (TSM) can work together hand in hand on either the same system or as separate products on different systems. In the first case, Tivoli Continuous Data Protection for Files cooperates directly with IBM Tivoli Storage Manager using the TSM support functionality for continuous remote or scheduled file protection. In the second case, Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager operate on different systems and we demonstrate that Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager can be used as an excellent complement to each other for the highest level of protecting the most valuable good of a modern business company: data.

We discuss this scenario by introducing a fictitious company named XYZ, Inc. Using this company as an example, we explain the configuration of Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager on different types of systems (mobile computers, workstations, and file server) so that the client can get the most benefit out of both products. We will also cover aspects that need some attention when configuring the TSM server.

Note: Let us quickly review the three main features of Tivoli Continuous Data Protection for Files (For more information, please refer to 1.3, “Main features of Tivoli Continuous Data Protection for Files” on page 12**)**:

- Continuous protection of high-importance files
- Real-time remote protection of high-importance files
- Scheduled backup to remote targets (all disk based and journal style) with versions to support point-in-time restore

As simple as those three main features sound, there are many various configuration possibilities of Tivoli Continuous Data Protection for Files, especially when combined with traditional backup solutions like, for example, IBM Tivoli Storage Manager.

The scenario described here is just one simple scenario out of many possible scenarios you can think of. It will be used to demonstrate the basic setup of Tivoli Continuous Data Protection for Files in combination with IBM Tivoli Storage Manager in a simplified and straightforward environment.

4.4.1 Overview

XYZ, Inc. is a medium sized business company using already IBM Tivoli Storage Manager (TSM) as the company’s backup solution for their main (file) servers. Not all workstation and mobile computer data are protected yet by IBM Tivoli Storage Manager. Due to the rapidly increasing number of viruses and other serious computer threats, XYZ, Inc. is afraid of losing data or facing any kind of data corruption (see 1.1.2, “Why Tivoli Continuous Data Protection for Files is needed” on page 4). They are now looking for an efficient and effective way to protect important data on their workstations and mobile computers, but can still continue using IBM Tivoli Storage Manager. The reason therefore is to secure the investments made already in IBM Tivoli Storage Manager.

A perfect product to fulfill the needs of XYZ, Inc. is Tivoli Continuous Data Protection for Files, as it can be used as a stand-alone product on end-user systems like workstations or mobile computers, and as a complement to traditional backup solutions like IBM Tivoli Storage Manager.

Note: XYZ, Inc. is a fictitious company and all similarities with real company names are coincidental.

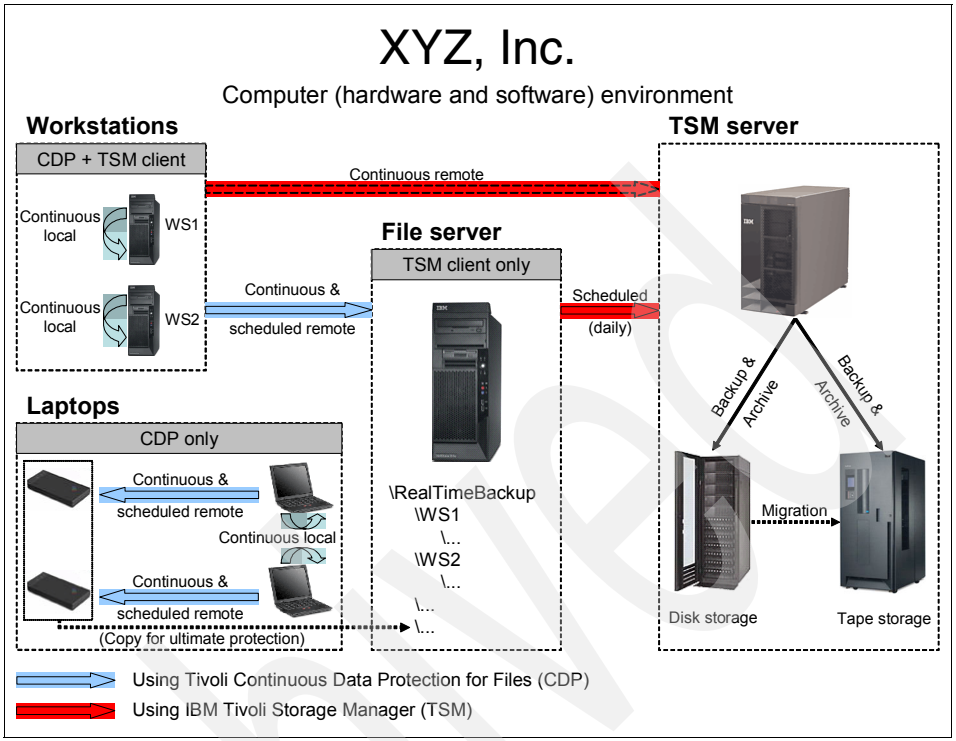


Figure 4-4 Overview about the computer environment of XYZ, Inc.

Figure 4-4 shows a simplified overview of the basic computer (hardware and software) environment of XYZ, Inc. using Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager. It consists mainly of four parts:

1. Mobile computers

   Mobile computers are used by mobile employees like, for example, sales people of XYZ, Inc. who spend most of their time outside the office travelling around the country. Tivoli Continuous Data Protection for Files is the only backup product being installed on these systems.

   A second partition (D:) on the internal hard drive will be used for continuos local backups of the most important files (local backup area). As the mobile computers are rarely connected to the company's network, the remote backup location for the high-importance files is not a file server but instead a removable disk like an external USB drive. To protect the rest of the mobile computer's files, a scheduled backup has been defined to store the data to the removable disk.

Note: As a removable drive can be lost, stolen, or unavailable in any other way, the files from the external disk can be copied (manually or via script) to the file server once the mobile computer is connected to the company's network again for ultimate data protection. In this case, the files from the mobile computer are also sent to the TSM server on a daily base using the TSM Backup/Archive client scheduler service running on the file server as an additional safeguard.

2. Workstations

   Workstations are connected to the company's network and used by the non-mobile employees of XYZ, Inc. On these systems, Tivoli Continuous Data Protection for Files has been installed as well as an optional TSM Backup/Archive client.

   The area for continuous local backups of the high important files is also, like on the mobile computers, a second partition (D:) on the internal hard drive. Due to the (mostly) permanent connection to the network of XYZ, Inc., the continuous remote backup location is a shared network drive on a file server especially set up for holding data of computers using Tivoli Continuous Data Protection for Files. The scheduled backups are defined to store the other workstation files on the same file server location on a daily base.

   Note: For additional protection, Tivoli Continuous Data Protection for Files can send files to a TSM server using the TSM Backup/Archive client being installed on the same system as Tivoli Continuous Data Protection for Files. Using both continuous remote backups to a file server *and* a TSM server at the same time might be too much in the sense of over-protecting data, but we will discuss it here in this scenario to show you how this can be realized.

   Please see "IBM Tivoli Storage Manager (TSM) server (Florence)" on page 160 for more details about the definitions that should be made on the TSM server concerning the TSM Backup/Archive clients running on the workstations.

3. File server

   The file server is the remote location for continuous and scheduled backups of Tivoli Continuous Data Protection for Files systems. On the file server itself, Tivoli Continuous Data Protection for Files is not installed, but only a TSM Backup/Archive client, a TSM scheduler service, and a TSM Backup/Archive Client Acceptor Daemon (CAD) to manage/control the scheduler service of the TSM Backup/Archive client. The file server will be backed up to a TSM

server once a day, usually during the night, according to a defined schedule on the TSM server.

Note: The file server is a dedicated server explicitly holding data from workstations or mobile computers running Tivoli Continuous Data Protection for Files. The reason is that we make, on the TSM server, some specific definitions for the TSM node name of the file server regarding versioning of files. In case other files would reside on the same file server, this would affect them as well, which might not (always) be wanted.

For more information about the specific definitions on the TSM server, please refer to “IBM Tivoli Storage Manager (TSM) server (Florence)” on page 160.

4. IBM Tivoli Storage Manager (TSM) server

   The IBM Tivoli Storage Manager (TSM) server is the final backup destination for long-time retention of data in the computer environment of XYZ, Inc. It receives the data being sent by the TSM Backup/Archive client (scheduler service) on the file server as well as the files from the TSM Backup/Archive client on the workstations. The TSM server is responsible for storing files on disk storage or tape storage, and for versioning and expiring files with respect to the policy settings being made.

   Note: It does not matter what operating system the TSM server is running on or what kind of storage (disk or tape) is being used to store the files. What is important are the policy definitions on the TSM server.

   Refer to “IBM Tivoli Storage Manager (TSM) server (Florence)” on page 160 for further details about the policy settings on the TSM server.

4.4.2 Details

This section covers details about the setup of each of the four main components (mobile computers, workstations, file server, and TSM server) of XYZ, Inc.’s computer environment and what definitions we have used in the ITSO lab for each one of them. The computer names, operating system versions, and TSM Backup/Archive client/server names we used in our lab were:

1. Mobile computer

   Name: Phoenix

   Operating system: Windows XP

2. Workstation

   Name: Cairo

   Operating system: Windows 2003

   TSM Backup/Archive client node name: CAIRO_WS

   TSM Backup/Archive client node password: CAIRO_WS

3. File server

   Name: Izmir

   Operating system: Windows 2003

   TSM Backup/Archive client node name: IZMIR_FS

   TSM Backup/Archive client node password: IZMIR_FS

4. IBM Tivoli Storage Manager (TSM) server

   Name: Florence

   Operating system: Windows 2003

   TSM server name: FLORENCE

This is summarized in Figure 4-5 on page 137, which gives a complete overview about the ITSO lab setup representing the computer (hardware and software) environment of XYZ, Inc.

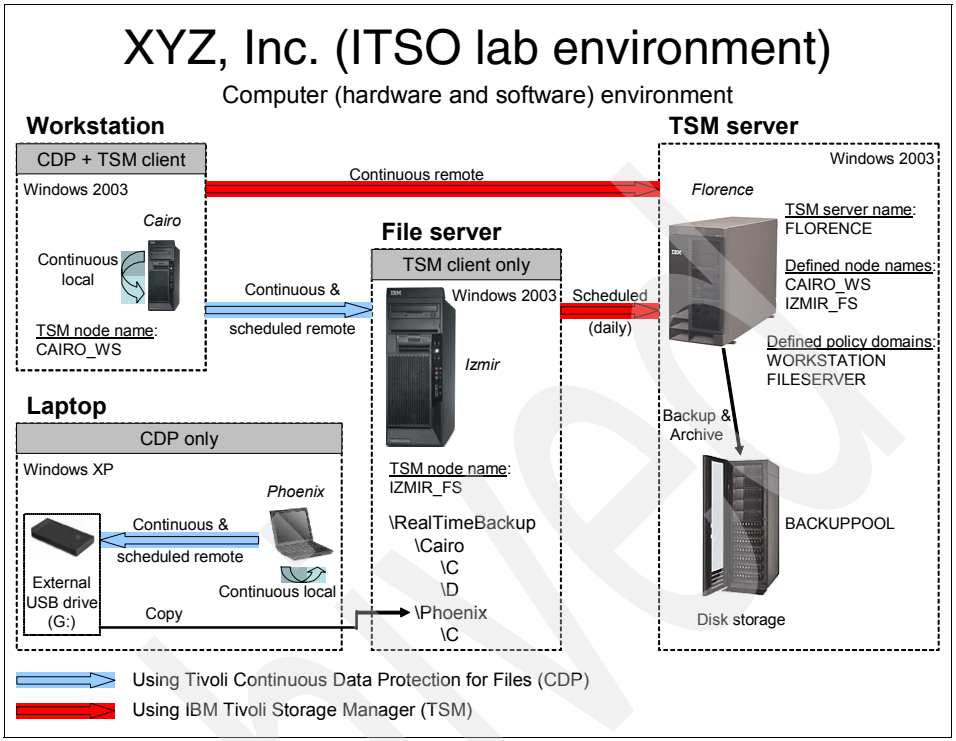


Figure 4-5 ITSO lab setup representing the computer environment of XYZ, Inc.

Mobile computer (Phoenix)

Tivoli Continuous Data Protection for Files is the only data protection software being installed on mobile computer Phoenix. The built-in (internal) disk is split into two partitions: drive C: and D:.

Drive C: is hosting the Windows XP operating system, the program files, and the standard folders, including My Documents, while general data is stored on the D: drive. The latter one is also the location of Tivoli Continuous Data Protection for Files' local backup area (RealTimeBackup folder), which is 5 GB in size. The backup location for continuous remote data protection is a removable disk (in this case, a USB drive with drive letter G: assigned), as the mobile computer is seldom connected to the network of XYZ, Inc. (see Figure 4-6).

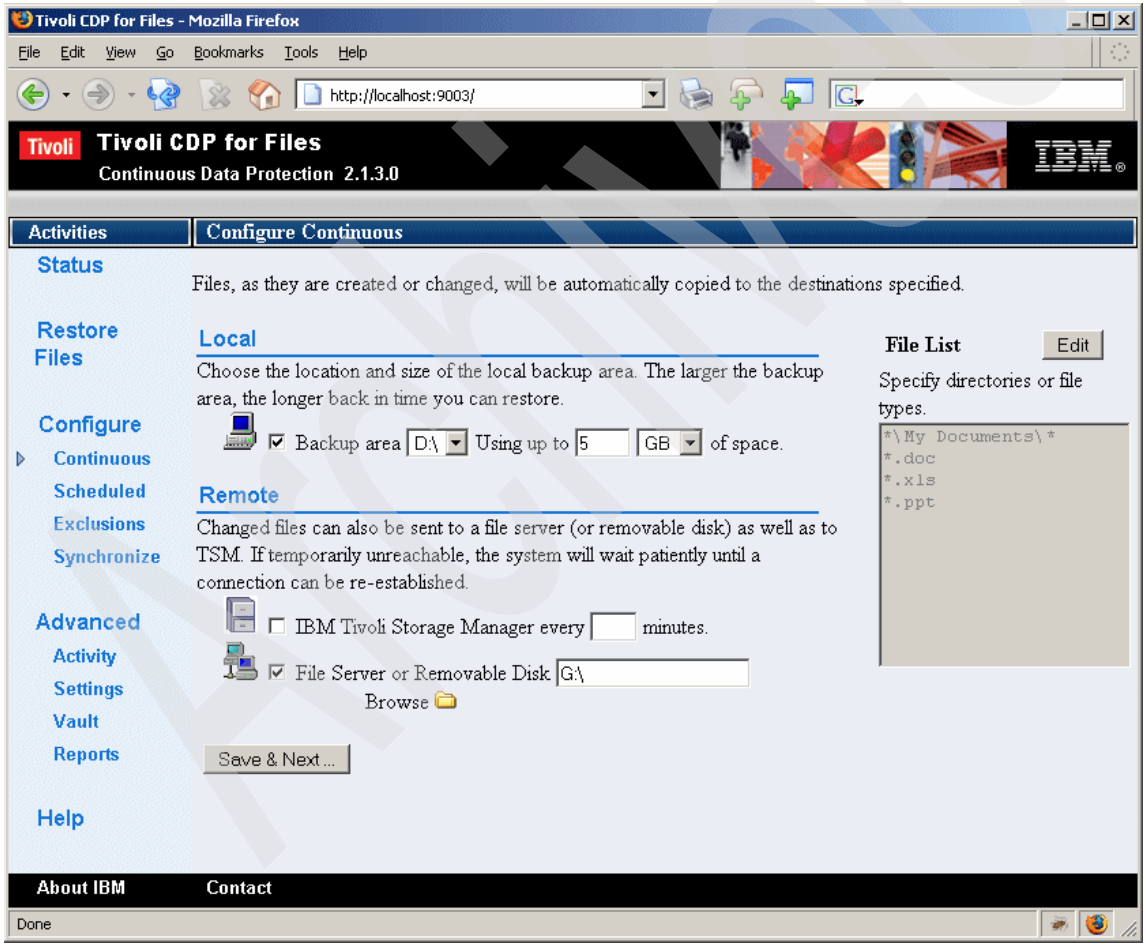


Figure 4-6 Continuous (local and remote) configuration of the mobile computer Phoenix

All files under any My Documents folder have been defined as highly important files as well as all Microsoft Word files (extension *.doc), Excel files (extension *.xls), and PowerPoint files (extension *.ppt), no matter where they are stored.

Figure 4-7 shows the schedule protection settings for mobile computer Phoenix. A daily schedule has been set up that saves all files (file list “*”), except the ones being excluded, to the external USB drive G:.

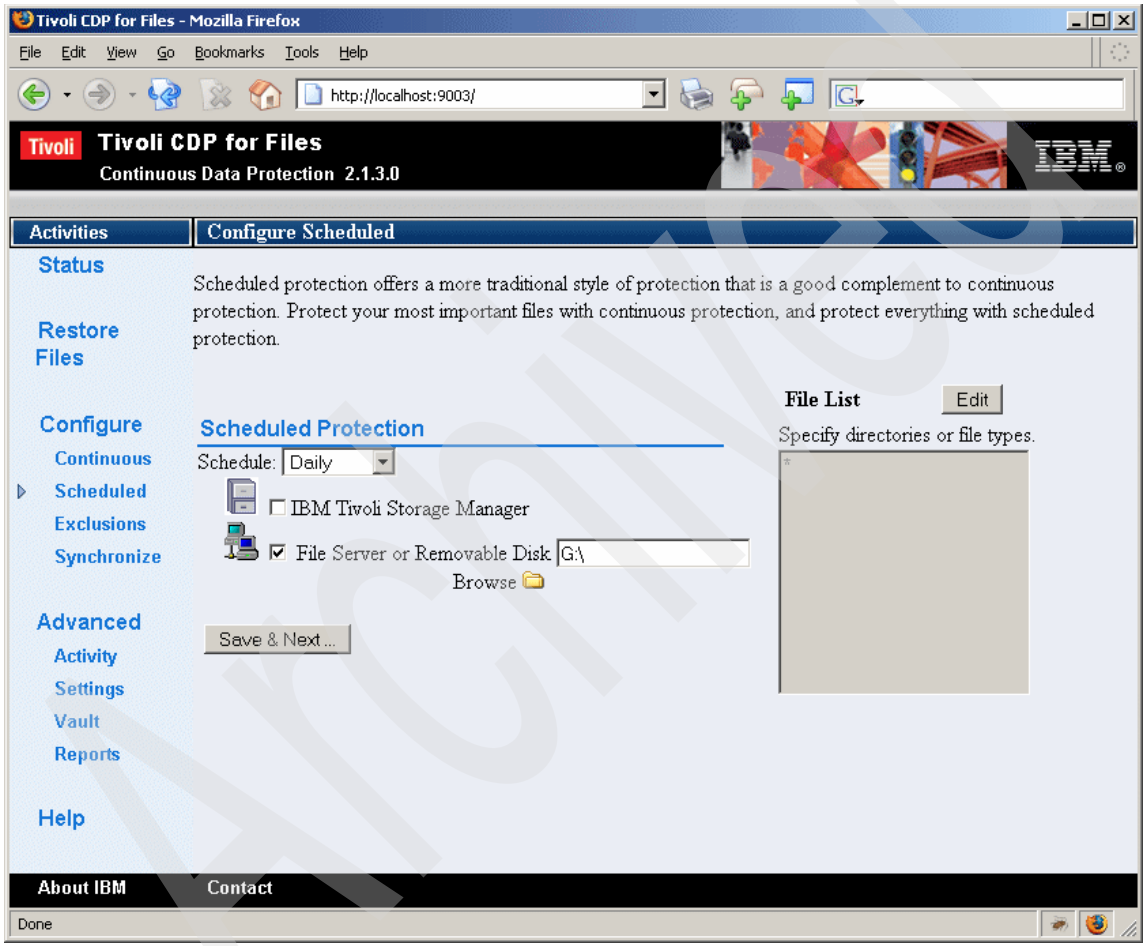


Figure 4-7 Scheduled configuration (daily schedule) of the mobile computer Phoenix

The Tivoli Continuous Data Protection for Files exclusion list has not been modified, so the standard exclusion list will be used, as seen in Figure 4-8.

```
RealTimeBackup
\Program Files
~
C:\WINDOWS\System32
*.tmp
*.temp
\Temp\
\Temporary
\Windows
\System Volume
\tsmlvsacache
\cache
```

Figure 4-8 Default exclusion list

Note: The list for defining the most important files, the scheduled file list, as well as the exclusion list, are highly flexible and can be edited to fit exactly your needs. As a general recommendation, you should use the default lists as a starting point and adjust the lists step by step until the wanted result is reached.

The remote space configuration setup of mobile computer Phoenix is displayed in Figure 4-9 on page 141. It shows that, at most, three versions per file will be stored in the (continuous) remote backup location on the external USB drive G:, occupying a maximum size of 30 GB. If the external USB drive is smaller than 30 GB, then this value needs to be lowered accordingly. If it is larger than 30 GB, this value allows you to store additional data on the external USB disk, for example, for sharing them with colleagues.

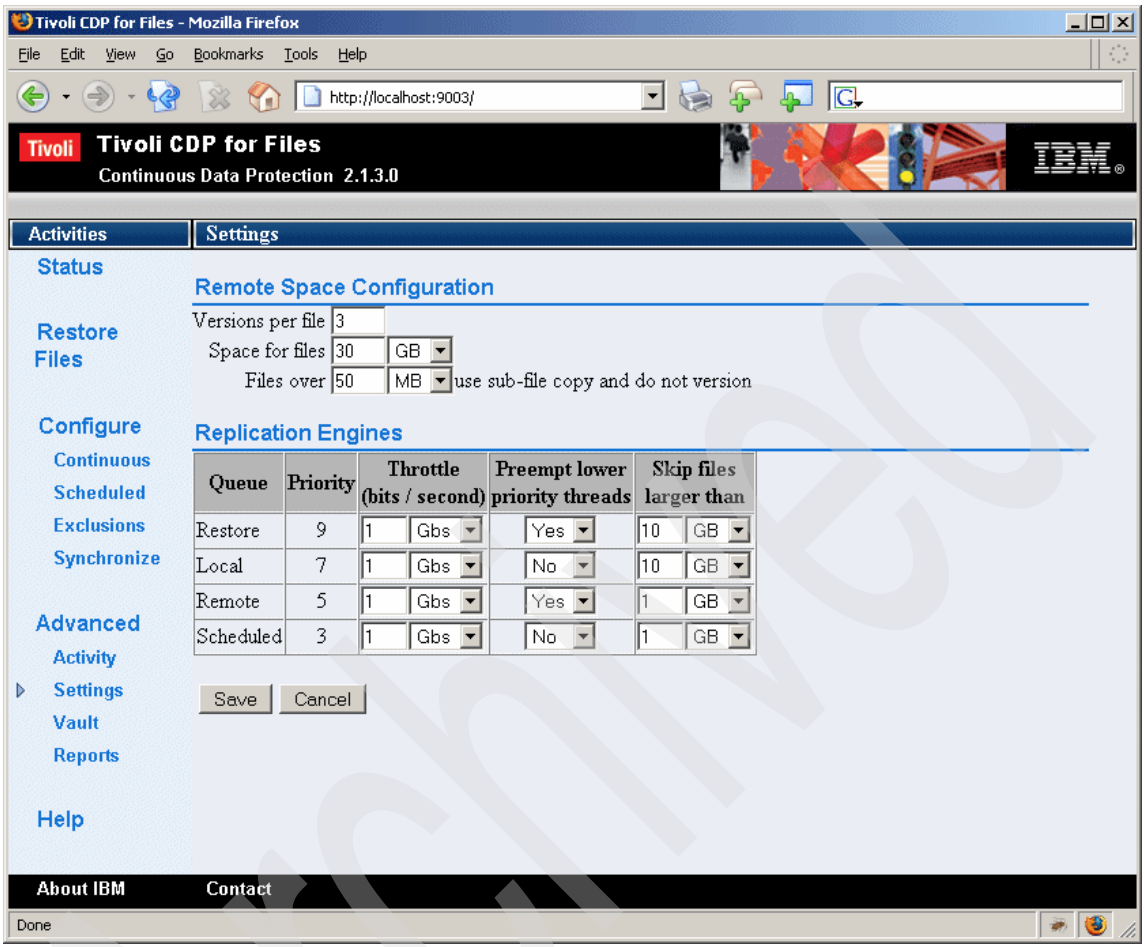


Figure 4-9 Remote space configuration (advanced settings) of mobile computer Phoenix

Figure 4-10 shows a Windows Explorer window of mobile computer Phoenix with the contents of internal drive D: (continuous local backup) and external USB drive G: (continuous remote and scheduled remote backup). For ultimate data protection, the directory named Phoenix under the RealTimeBackup folder on drive G: can be copied (manually or scripted) to file server Izmir once mobile computer Phoenix is connected to the network of XYZ, Inc. again. If so, the data of mobile computer Phoenix will be finally stored on the TSM server too, by virtue of the daily TSM Backup/Archive client scheduler service running on file server Izmir (see “File server (Izmir)” on page 150 for more details).

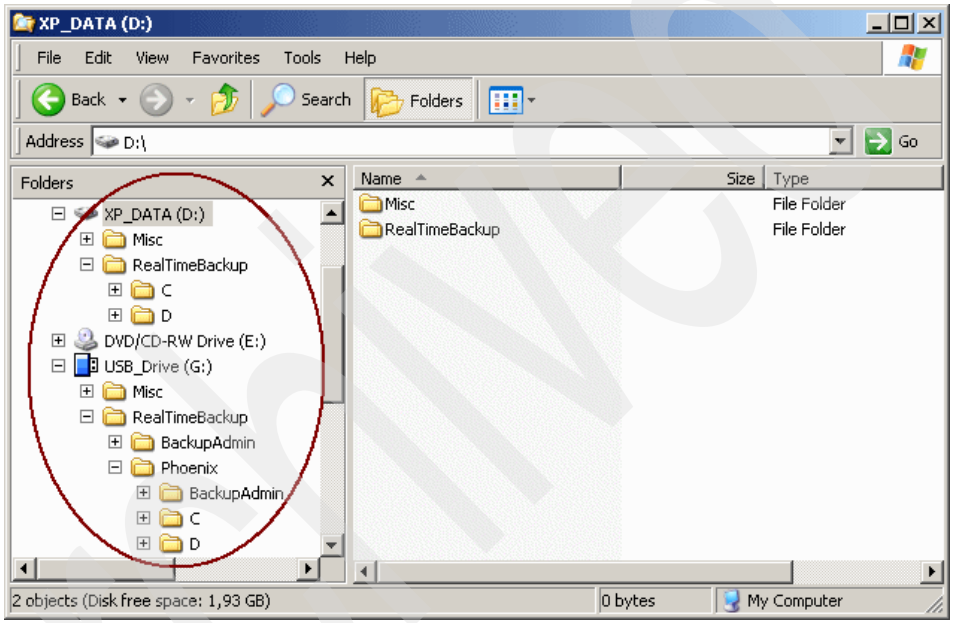


Figure 4-10 Contents of internal drive D: (XP_DATA) and external USB drive G: (USB_Drive)

Workstation (Cairo)

Beside Tivoli Continuous Data Protection for Files, there is also an IBM Tivoli Storage Manager (TSM) Backup/Archive client installed on workstation Cairo for additional data protection.

Note: We do not describe here in detail how to install and configure the TSM Backup/Archive client. For more information about this, please refer to *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788. We assume that the TSM Backup/Archive client has already been installed successfully on workstation Cairo.

Setup of Tivoli Continuous Data Protection for Files

As on mobile computer Phoenix, the internal disk of workstation Cairo is divided into a C: and D: partition (drives).

The Windows 2003 operating system, the program files, and the standard folders, including My Documents, are installed on the C: drive, while drive D: is used for common data and general files being worked on. The backup area (RealTimeBackup folder) for continuous local protection is 10 GB in size and is also stored on the D: drive. For continuous remote data protection, two remote backup locations have been specified:

- An IBM Tivoli Storage Manager (TSM) server (Florence)

  Every 60 minutes, highly important files that have been changed will be backed up to TSM server Florence using the installed TSM Backup/Archive client.

- A shared network folder on a remote file server (Izmir)

  As soon as a file changes that has been defined a high-importance file, it will be stored on shared network folder e$ on file server Izmir (\\izmir\e$).

Figure 4-11 shows the continuous (local and remote) configuration menu of the Tivoli Continuous Data Protection for Files GUI for workstation Cairo.

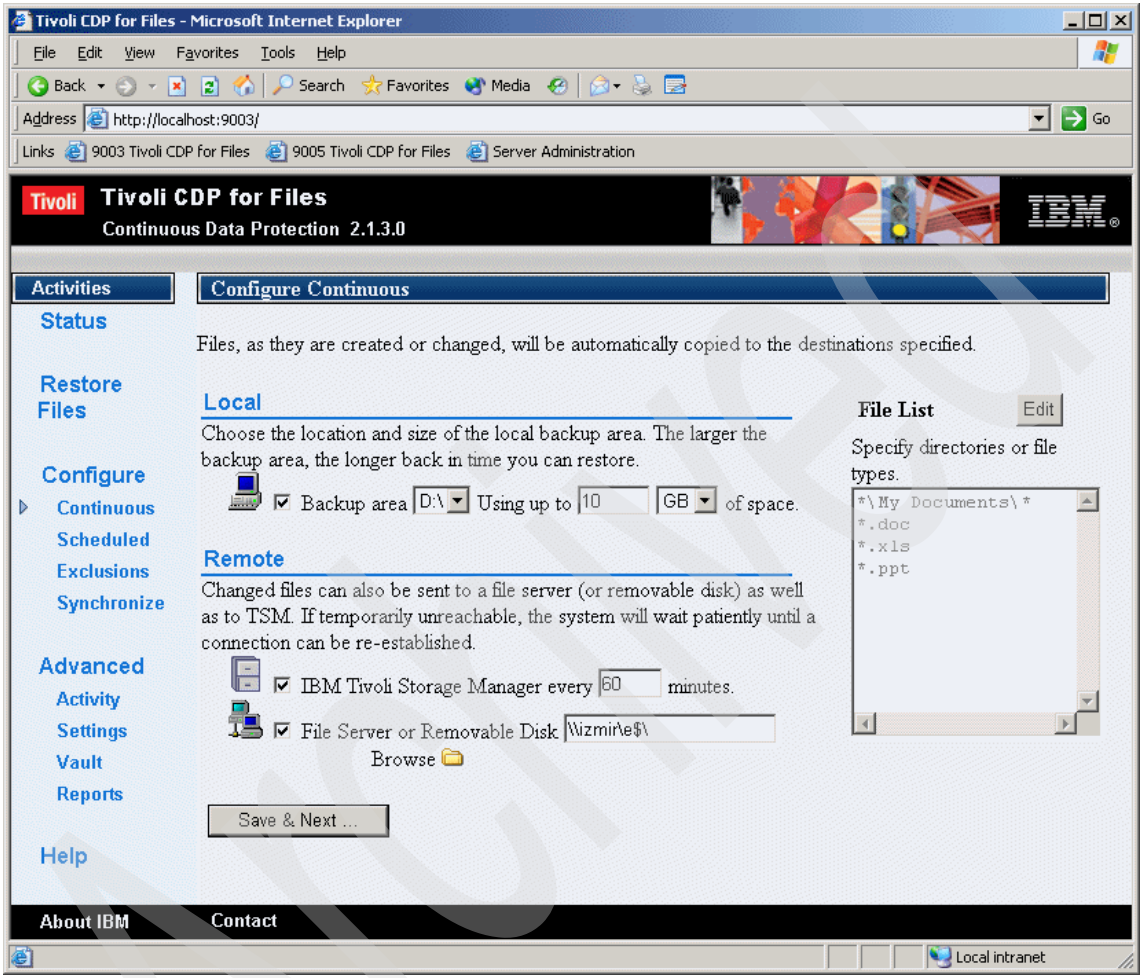


Figure 4-11 Continuous (local and remote) configuration of workstation Cairo

As the most important files to protect continuously, all files in any My Documents folder and all Microsoft Office files (extensions *.doc, *.xls and *.ppt), independent from their storage location, have been defined.

The scheduled configuration settings for workstation Cairo is displayed in Figure 4-12 on page 145. All files (file list "*"), except the ones being excluded from protection by the default exclusion list (see Figure 4-8 on page 140), will be sent to shared network folder e$ on file server Izmir (\\izmir\e$) based on a daily schedule.

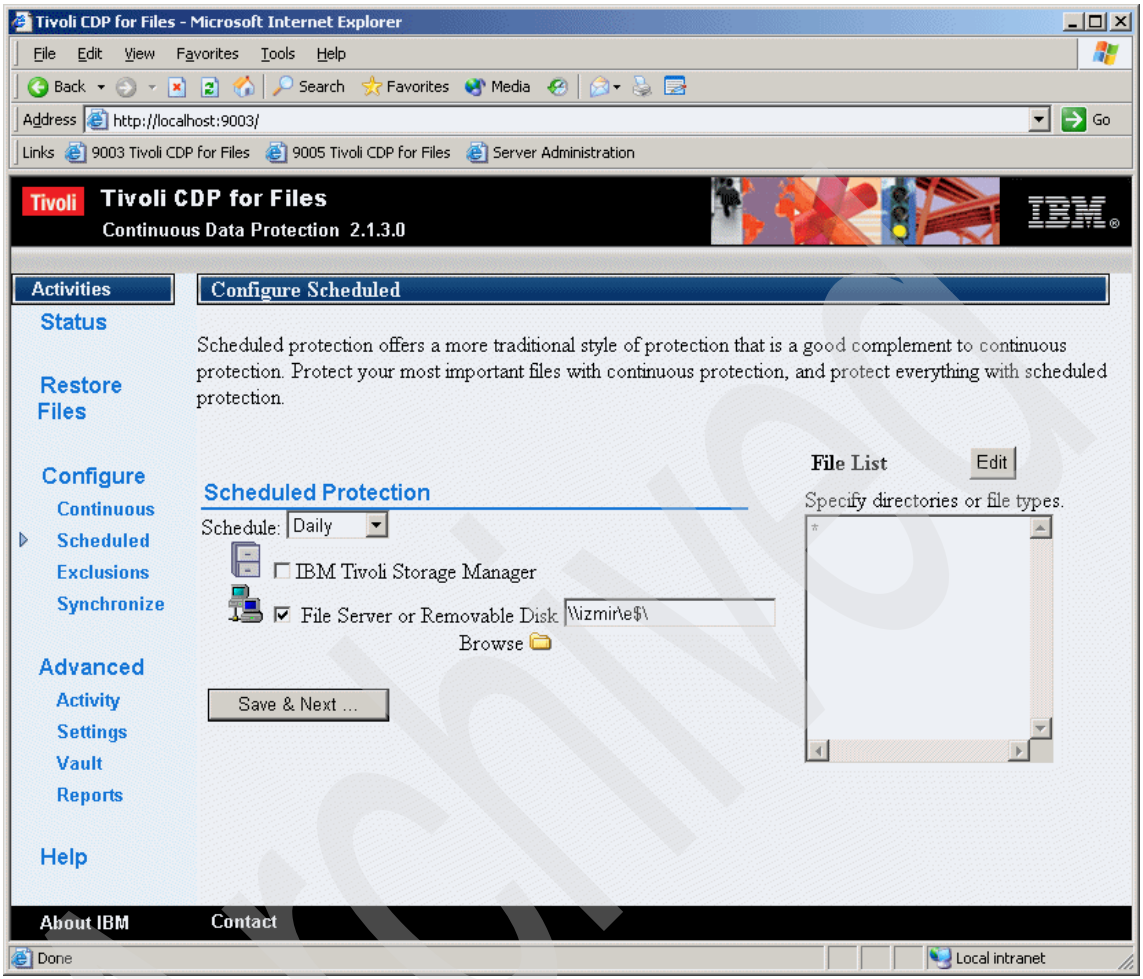


Figure 4-12 Scheduled configuration (daily schedule) of workstation Cairo

Figure 4-13 shows the Tivoli Continuous Data Protection for Files GUI with the remote space configuration settings of workstation Cairo. We defined to store at most five versions per file occupying a maximum size of 50 GB on file server Izmir. These numbers are higher compared to mobile computer Phoenix, as file server Izmir has a comparatively higher disk storage capacity per Tivoli Continuous Data Protection for Files system than the external USB drive used by mobile computer Phoenix.

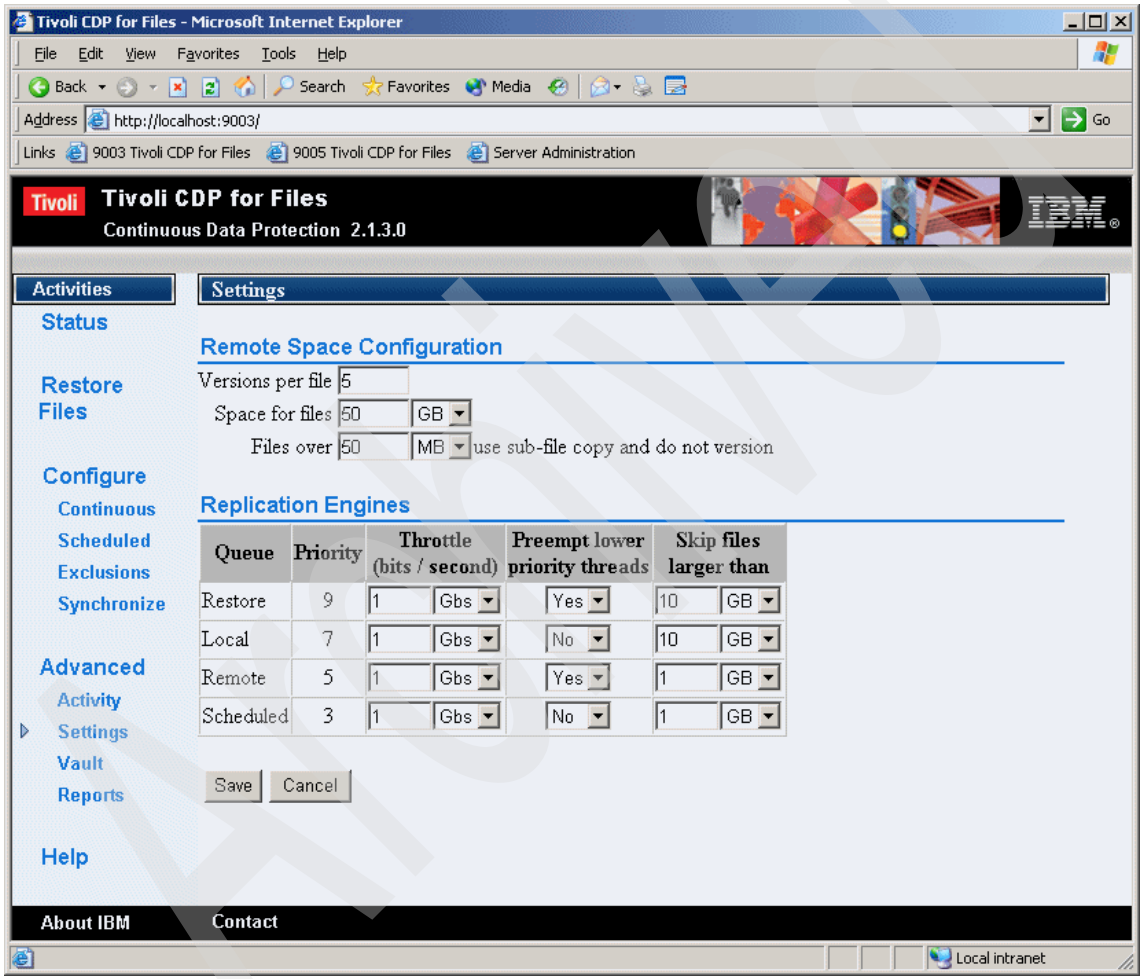


Figure 4-13 Remote space configuration (advanced settings) of workstation Cairo

In Figure 4-14 on page 147, you can see a Windows Explorer window of workstation Cairo displaying the contents of internal drive D: (continuous local backup) and shared network folder e$ on file server Izmir (continuous remote and scheduled remote backup).

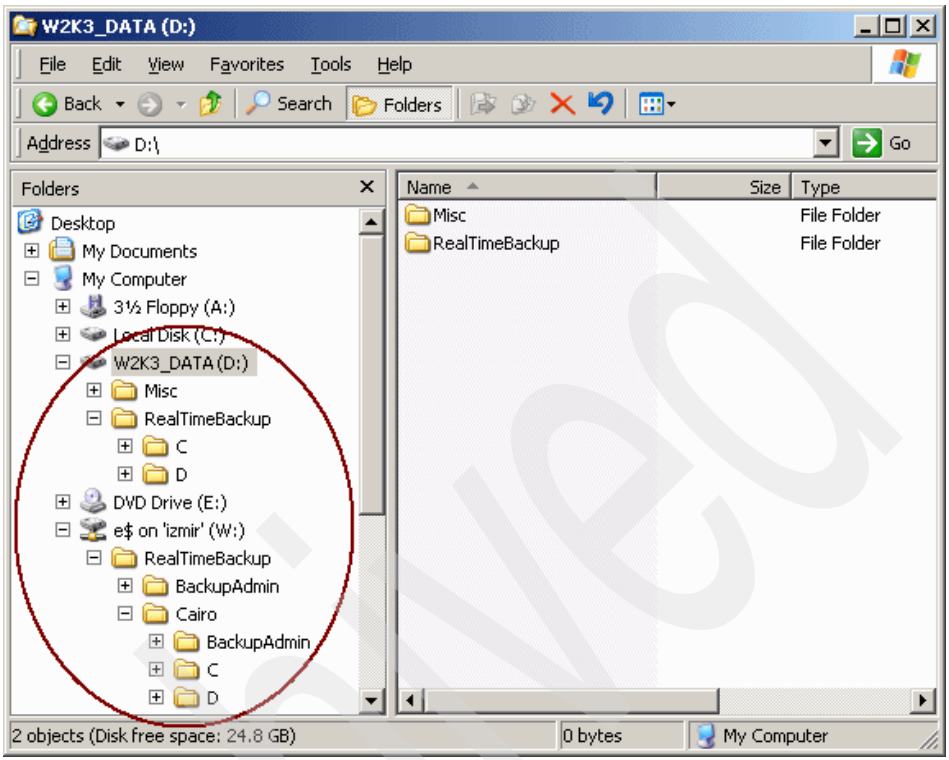


Figure 4-14 Windows Explorer showing the contents of internal drive D: (W2K3_DATA) and remote backup location on file server Izmir (\\izmir\e$)

Note: Directly beneath the RealTimeBackup folder on file server Izmir (remote backup location), Tivoli Continuous Data Protection for Files created automatically a unique folder with the computer's network name (*Cairo*) at the top of the directory structure. This allows multiple computers to use the same remote backup location (\\izmir\e$) but still have a strict separation between each computer's files.

IBM Tivoli Storage Manager (TSM) Backup/Archive client setup

The IBM Tivoli Storage Manager (TSM) Backup/Archive client installed on workstation Cairo is only used for continuous remote backups by Tivoli Continuous Data Protection for Files (see Figure 4-11 on page 144). As we have already set up a daily schedule (see Figure 4-12 on page 145) using Tivoli Continuous Data Protection for Files, there is no need to install an additional TSM Backup/Archive client scheduler service on workstation Cairo.

In this case, the TSM Backup/Archive client options file dsm.opt can be kept rather small and simple. Example 4-1 shows the dsm.opt file being used by workstation Cairo: It contains the minimal needed TSM client options as well as a minimum TSM include/exclude list.

Example 4-1 TSM Backup/Archive client options file (dsm.opt) of workstation Cairo

```
*
* DSM.OPT file for workstation CAIRO
*
COMMMethod         TCPip
TCPServeraddress   florence
TCPPort            1500
NODename           CAIRO_WS
PASSWORDAccess     generate
*
* TSM include/exclude list
*
Exclude "*:\microsoft uam volume\...\*"
Exclude "*:\microsoft uam volume\...\*.*"
Exclude *:\...\pagefile.sys
Exclude *:\MSDOS.SYS
Exclude *:\IO.SYS
Exclude *:\...\system32\config\...\*
Exclude *:\...\system32\Perflib*.dat
Exclude *:\...\system32\dhcp\...\*
Include *:\...\system32\dhcp\backup\...\*
Exclude *:\...\system32\dns\...\*
Include *:\...\system32\dns\backup\...\*
Exclude.dir "*:\System Volume Information"
Exclude.dir "*:\...\Temporary Internet Files"
Exclude.dir *:\Recycled
Exclude.dir *:\Recycler
```

Important: Please make sure to specify the `PASSWORDAccess generate` option in the dsm.opt file. Otherwise, the TSM Backup/Archive command-line client (dsmc.exe) will *hang as a background process* waiting for you to enter a user ID and password once it has been started by Tivoli Continuous Data Protection for Files.

For more information, please refer to 3.3.2, “Passwordaccess generate versus passwordaccess prompt” on page 82.

Before Tivoli Continuous Data Protection for Files can send files to TSM server Florence using the TSM Backup/Archive client, the TSM client node, in this case CAIRO_WS, needs to be registered on the TSM server.

Note: How to register a TSM client node will be discussed later on when we talk about TSM server Florence and its policy definitions (see “Register TSM client nodes CAIRO_WS and IZMIR_FS” on page 167).

Once TSM client node name CAIRO_WS has been registered on TSM server Florence, the TSM Backup/Archive client on workstation Cairo needs to be started manually at least one time to enter the user ID and password, which then will be stored encrypted into the Windows registry. If this has been done, the necessary information will be taken from the Windows registry without prompting for a user ID and password again each time the TSM Backup/Archive client is started.

To manually start the TSM Backup/Archive command-line client, please do the following:

1. Select **Start** → **Run**, type **cmd**, and click **OK**. A Windows command-line window appears.
2. To change to the installation directory of the TSM Backup/Archive client, enter **cd “\program files\tivoli\tsm\baclient”**.
3. To start the TSM Backup/Archive command-line client, enter **dsmc**.
4. When prompted for your user ID, type CAIRO_WS or just press Enter.
5. When prompted for your password, type the password CAIRO_WS for the user ID (node name) and press Enter.
6. To stop the TSM Backup/Archive command-line client again, use the **quit** command.
7. To close the Windows command-line window, type **exit**.

Example 4-2 shows the initial TSM Backup/Archive command-line client session for TSM client node CAIRO_WS after it has been registered on TSM server Florence.

Example 4-2 TSM Backup/Archive command-line client session for TSM node CAIRO_WS

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\program files\tivoli\tsm\baclient"

C:\Program Files\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 3, Level 2.0
  Client date/time: 04/07/2006 15:04:55
(c) Copyright by IBM Corporation and other(s) 1990, 2005. All Rights Reserved.

Node Name: CAIRO_WS
Please enter your user id <CAIRO_WS>: CAIRO_WS

Please enter password for user id "CAIRO_WS": ********

Session established with server FLORENCE: Windows
  Server Version 5, Release 3, Level 2.0
  Server date/time: 04/07/2006 15:03:41  Last access: 04/07/2006 15:03:41

tsm> quit

C:\Program Files\Tivoli\TSM\baclient>
```

After the password has been stored successfully in the Windows registry of workstation Cairo, Tivoli Continuous Data Protection for Files can use the TSM Backup/Archive command-line client for backing up files to TSM server Florence for continuous remote data protection.

File server (Izmir)

File server Izmir is a dedicated server explicitly holding data from workstations (like Cairo) or mobile computers (like Phoenix) using Tivoli Continuous Data Protection for Files. It does so by sharing drive E: (share name e$) in the network of XYZ, Inc., so that computers running Tivoli Continuous Data Protection for Files can use this network drive as their remote backup location.

Figure 4-15 on page 151 displays the contents of shared network drive E: (CDP_Data) on file server Izmir.

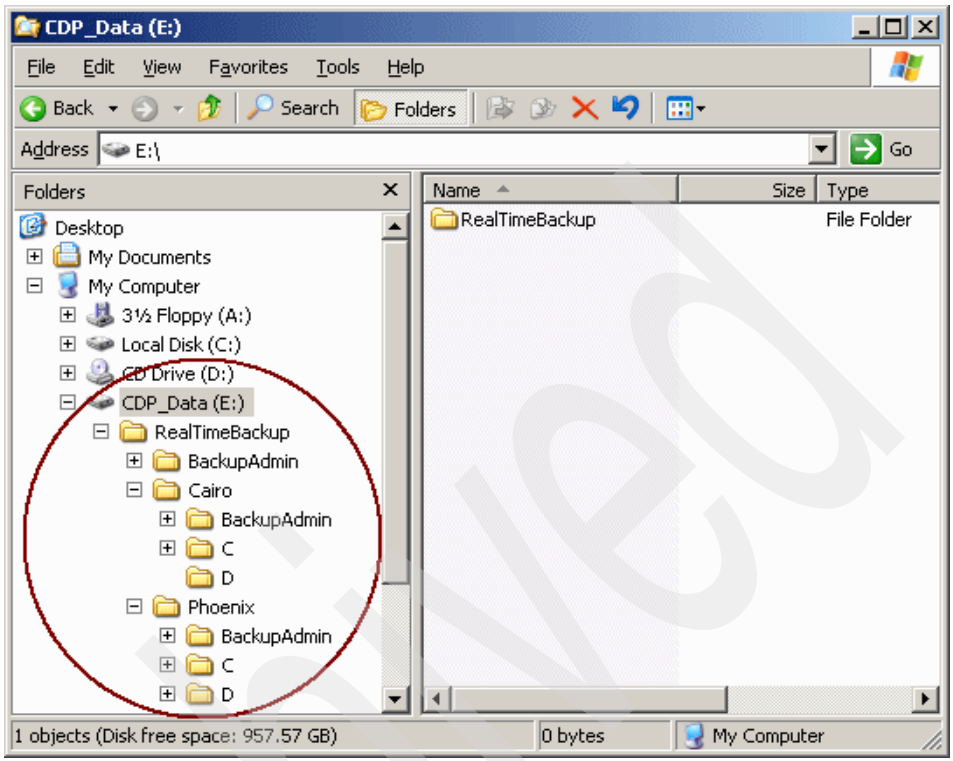


Figure 4-15 Contents of shared drive E: (CDP_Data) on file server Izmir

Note:

- Folder \RealTimeBackup\Cairo *has been* created automatically on this drive as we have defined Tivoli Continuous Data Protection for Files on Cairo to use the shared network folder e$ on Izmir as its remote backup destination for continuous remote and scheduled remote data protection (see “Workstation (Cairo)” on page 142).
- Folder \RealTimeBackup\Phoenix *has not been* created automatically on the shared network drive e$ on Izmir due to the definitions we have made for Tivoli Continuous Data Protection for Files on Phoenix. It has been copied from the external USB drive of Phoenix once the mobile computer has been connected to the network of XYZ, Inc. again (see “Mobile computer (Phoenix)” on page 138).

Tivoli Continuous Data Protection for Files itself is not running on file server Izmir. Instead, a IBM Tivoli Storage Manager (TSM) Backup/Archive client, a TSM scheduler service, and a TSM Backup/Archive Client Acceptor Daemon (CAD) to manage/control the scheduler service of the TSM Backup/Archive client are installed on the file server.

The TSM Backup/Archive client and the TSM scheduler service respectively are ultimately responsible for storing all the data of XYZ, Inc.'s computer environment residing on shared network drive e$ on Izmir for long-time retention on TSM server Florence.

The file dsm.opt used by the TSM Backup/Archive client, the TSM scheduler service, and the CAD on file server Izmir can be seen in Example 4-3.

Example 4-3 TSM Backup/Archive client options file (dsm.opt) of file server Izmir

```
*
* DSM.OPT file for file server IZMIR
*
COMMMethod         TCPip
TCPServeraddress   florence
TCPPort            1500
NODename           IZMIR_FS
PASSWORDAccess     generate
*
* Domain statement to backup only drive E:
*
DOMain             E:
*
* Settings to use CAD for scheduler
*
MANAGEDServices   schedule
*
* TSM include/exclude list
*
Exclude "*:\...\*"
Include "*:\...\RealTimeBackup\...\*"
Exclude.dir "*:\System Volume Information"
Exclude.dir *:\Recycled
Exclude.dir *:\Recycler
```

Compared to the dsm.opt file of workstation Cairo, two additional TSM client options have been added: DOMain and MANAGEDServices. Table 4-1 on page 153 provides a short description and the default values for options DOMain and MANAGEDServices, if not explicitly set in the TSM Backup/Archive client options file.

Table 4-1 Explanation of TSM Backup/Archive client options DOMain and MANAGEDServices

Option	Description	Default value (if not set)
DOMain	The domain option specifies the drives that you want to include for incremental backup in your client domain.	all-local
MANAGEDServices	The managedservices option specifies whether the Tivoli Storage Manager Client Acceptor service (CAD) manages the scheduler, the Web client, or both.	webclient

Specifying DOMain E: prevents all local drives of file server Izmir to be backed up incrementally by the TSM Backup/Archive client. Instead, incremental backups are limited to shared network drive E: only, where all the Tivoli Continuous Data Protection for Files' data is stored on.

Using the CAD to manage the TSM scheduler service can provide several benefits, where MANAGEDServices schedule has been added to the dsm.opt file:

- Memory retention problems that may occur when using traditional methods of running the scheduler are resolved. Using the CAD to manage the scheduler requires very little memory between scheduled operations.
- The CAD can manage both the scheduler program and the Web client, reducing the number of background processes on your workstation.

A minimum TSM include/exclude list has been defined in dsm.opt as well. It *includes all files and directories under the RealTimeBackup folder* (`Include "*:\...\RealTimeBackup\...\*"`) for backup processing, but *excludes all other files* (`Exclude "*:\...\*"`) on shared network drive E:, if there are any, to be backed up.

After TSM client node IZMIR_FS has been registered on TSM server Florence (please refer to "Register TSM client nodes CAIRO_WS and IZMIR_FS" on page 167 for more information about registering a TSM client node), the TSM Backup/Archive client on file server Izmir needs to be started manually at least one time to enter the user ID and password, which then will be stored encrypted into the Windows registry.

To manually start the TSM Backup/Archive command-line client, please do the following:

1. Select **Start** → **Run**, type **cmd**, and click **OK**. A Windows command-line window appears.
2. To change to the installation directory of the TSM Backup/Archive client, enter **cd "\program files\tivoli\tsm\baclient"**.
3. To start the TSM Backup/Archive command-line client, enter **dsmc**.
4. When prompted for your user ID, type IZMIR_FS or just press Enter.
5. When prompted for your password, type the password IZMIR_FS for the user ID (node name) and press Enter.
6. To stop the TSM Backup/Archive command-line client again, use the **quit** command.
7. To close the Windows command-line window, type **exit**.

If this has been done, the necessary information will be taken from the Windows registry without prompting for a user ID and password again each time the TSM Backup/Archive client is started.

The TSM Backup/Archive command-line client session for TSM client node IZMIR_FS, after it has been registered on TSM server Florence, is shown in Example 4-4.

Example 4-4 TSM Backup/Archive command-line client session for TSM node IZMIR_FS

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\program files\tivoli\tsm\baclient"

C:\Program Files\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 3, Level 2.0
  Client date/time: 04/07/2006 15:07:47
(c) Copyright by IBM Corporation and other(s) 1990, 2005. All Rights Reserved.

Node Name: IZMIR_FS
Please enter your user id <IZMIR_FS>: IZMIR_FS

Please enter password for user id "IZMIR_FS": ********

Session established with server FLORENCE: Windows
  Server Version 5, Release 3, Level 2.0
  Server date/time: 04/07/2006 15:07:03  Last access: 04/07/2006 15:07:02
```

```
tsm> quit

C:\Program Files\Tivoli\TSM\baclient>
```

Once the TSM Backup/Archive client has contacted TSM server Florence and the password has been stored in the Windows registry, the TSM scheduler service and TSM Backup/Archive Client Acceptor Daemon (CAD) need to be installed. This can be done either via the setup wizard of the TSM Backup/Archive GUI (dsm.exe) or the TSM Client Service Configuration Utility (dsmcutil.exe).

- To start the setup wizard, select **Utilities** → **Setup Wizard** from the TSM Backup/Archive client GUI, and you will be guided by the configuration wizard through the installation process.
- To use the TSM Client Service Configuration Utility, please do the following:
  - Select **Start** → **Run**, type **cmd**, and click **OK**. A Windows command-line window appears.
  - To change to the installation directory of the TSM Backup/Archive client, enter **cd "\program files\tivoli\tsm\baclient"**.
  - To install the TSM scheduler service, enter **dsmcutil install scheduler /name:"TSM Scheduler Service" /clientdir:"c:\program files\tivoli\TSM\baclient" /optfile:"c:\program files\tivoli\TSM\baclient\dsm.opt" /node:IZMIR_FS /password:IZMIR_FS /autostart:yes /startnow:no**.
  - To install the TSM Backup/Archive Client Acceptor Daemon (CAD), type **dsmcutil install CAD /name:"TSM Client Acceptor" /clientdir:"c:\program files\tivoli\TSM\baclient" /optfile:"c:\program files\tivoli\TSM\baclient\dsm.opt" /node:IZMIR_FS /password:IZMIR_FS /cadschedname:"TSM Scheduler Service" /autostart:yes /startnow:no**.
  - Manually start the CAD with **dsmcutil start /name:"TSM Client Acceptor"**.
  - To close the Windows command-line window, type **exit**.

Example 4-5 displays the installation of the TSM scheduler service and TSM Backup/Archive Client Acceptor Daemon (CAD) using the TSM Client Service Configuration Utility. In addition to the **dsmcutil install** commands, it shows also the **dsmcutil list** command outputs, which lists the (installed) TSM client services before and after their installation.

Example 4-5 Installation of TSM Client Acceptor Daemon (CAD) and TSM scheduler service using dsmcutil

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\program files\tivoli\tsm\baclient"

C:\Program Files\Tivoli\TSM\baclient>dsmcutil list

TSM Windows NT Client Service Configuration Utility
Command Line Interface - Version 5, Release 3, Level 2.0
(C) Copyright IBM Corporation, 1990, 2005, All Rights Reserved.
Last Updated Sep 17 2005
TSM Api Verison 5.3.2

Command: List Installed TSM Client Services
Machine: IZMIR(Local Machine)



No TSM Client Services were located.


C:\Program Files\Tivoli\TSM\baclient>dsmcutil install scheduler /name:"TSM Scheduler Service"
/clientdir:"c:\program files\tivoli\TSM\baclient" /optfile:"c:\program
files\tivoli\TSM\baclient\dsm.opt" /node:IZMIR_FS /password:IZMIR_FS /autostart:yes
/startnow:no

TSM Windows NT Client Service Configuration Utility
Command Line Interface - Version 5, Release 3, Level 2.0
(C) Copyright IBM Corporation, 1990, 2005, All Rights Reserved.
Last Updated Sep 17 2005
TSM Api Verison 5.3.2

Command: Install TSM Client Service
Machine: IZMIR(Local Machine)



Installing TSM Client Service:

       Machine          : IZMIR
       Service Name     : TSM Scheduler Service
```

```
       Client Directory : c:\program files\tivoli\TSM\baclient
       Automatic Start  : yes
       Logon Account    : LocalSystem

The service was successfully installed.


Creating Registry Keys ...

Updated registry value 'ImagePath' .
Updated registry value 'EventMessageFile' .
Updated registry value 'TypesSupported' .
Updated registry value 'TSM Scheduler Service' .
Updated registry value 'ADSMClientKey' .
Updated registry value 'OptionsFile' .
Updated registry value 'EventLogging' .
Updated registry value 'ClientNodeName' .

Generating registry password ...
Authenticating TSM password for node IZMIR_FS ...

Connecting to TSM Server via client options file 'c:\program files\tivoli\TSM\baclient\dsm.opt'
...

Password authentication successful.

The registry password for TSM node IZMIR_FS has been updated.


C:\Program Files\Tivoli\TSM\baclient>dsmcutil install CAD /name:"TSM Client Acceptor"
/clientdir:"c:\program files\tivoli\TSM\baclient" /optfile:"c:\program
files\tivoli\TSM\baclient\dsm.opt" /node:IZMIR_FS /password:IZMIR_FS /cadschedname:"TSM
Scheduler Service" /autostart:yes /startnow:no

TSM Windows NT Client Service Configuration Utility
Command Line Interface - Version 5, Release 3, Level 2.0
(C) Copyright IBM Corporation, 1990, 2005, All Rights Reserved.
Last Updated Sep 17 2005
TSM Api Verison 5.3.2

Command: Install TSM Client Service
Machine: IZMIR(Local Machine)



Installing TSM Client Service:

       Machine          : IZMIR
       Service Name     : TSM Client Acceptor
```

```
       Client Directory : c:\program files\tivoli\TSM\baclient
       Automatic Start  : yes
       Logon Account    : LocalSystem

The service was successfully installed.


Creating Registry Keys ...

Updated registry value 'ImagePath' .
Updated registry value 'EventMessageFile' .
Updated registry value 'TypesSupported' .
Updated registry value 'TSM Client Acceptor' .
Updated registry value 'ADSMClientKey' .
Updated registry value 'OptionsFile' .
Updated registry value 'EventLogging' .
Updated registry value 'ClientNodeName' .
Updated registry value 'CadSchedName' .

Generating registry password ...
Authenticating TSM password for node IZMIR_FS ...

Connecting to TSM Server via client options file 'c:\program files\tivoli\TSM\baclient\dsm.opt'
...

Password authentication successful.

The registry password for TSM node IZMIR_FS has been updated.


C:\Program Files\Tivoli\TSM\baclient>dsmcutil list

TSM Windows NT Client Service Configuration Utility
Command Line Interface - Version 5, Release 3, Level 2.0
(C) Copyright IBM Corporation, 1990, 2005, All Rights Reserved.
Last Updated Sep 17 2005
TSM Api Verison 5.3.2

Command: List Installed TSM Client Services
Machine: IZMIR(Local Machine)


Installed TSM Client Services:

   1. TSM Client Acceptor
   2. TSM Scheduler Service

2 TSM Client Services were located.
```

```
C:\Program Files\Tivoli\TSM\baclient>dsmcutil start /name:"TSM Client Acceptor"

TSM Windows NT Client Service Configuration Utility
Command Line Interface - Version 5, Release 3, Level 2.0
(C) Copyright IBM Corporation, 1990, 2005, All Rights Reserved.
Last Updated Sep 17 2005
TSM Api Verison 5.3.2

Command: Start TSM Client Service
Machine: IZMIR(Local Machine)


Starting the 'TSM Client Acceptor' service ...

The service was successfully started.


C:\Program Files\Tivoli\TSM\baclient>
```

After the TSM scheduler service and TSM Backup/Archive Client Acceptor Daemon (CAD) have been installed, they appear as Windows services in the administrative tool Services. Depending on the Windows operating system, follow these steps to start Services:

- Windows XP:

  Select **Start** → **Control window** → **Administrative Tools** → **Services**.

- Windows 2000 and 2003:

  Select **Start** → **Settings** → **Control window** → **Administrative Tools** → **Services**.

The installed TSM client services can be seen in Figure 4-16.

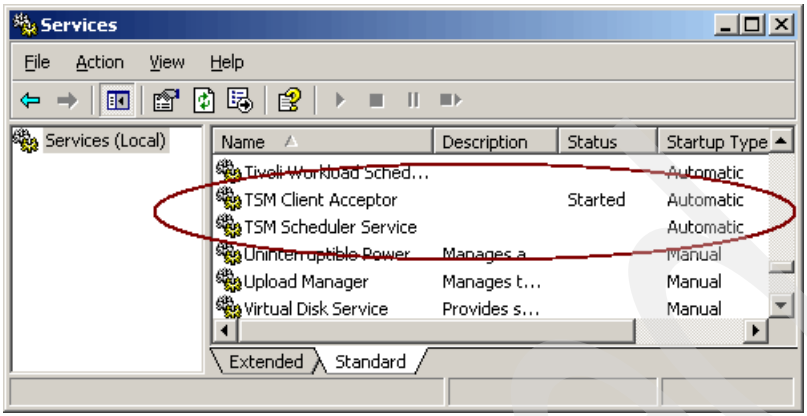


Figure 4-16 TSM Client Acceptor Daemon (CAD) and TSM scheduler service

The final step to protect file server Izmir is to define a TSM client schedule on TSM server Florence, which runs an incremental backup of TSM node IZMIR_FS on a daily base. How to do so will be discussed in “Define TSM client schedule for node IZMIR_FS” on page 168.

IBM Tivoli Storage Manager (TSM) server (Florence)

IBM Tivoli Storage Manager (TSM) server Florence receives the data being sent by the TSM Backup/Archive client (scheduler service) on file server Izmir as well as the files from the TSM Backup/Archive client on workstation Cairo and is therefore the final backup destination for long-time data retention in the computer environment of XYZ, Inc.

Policy domain definitions WORKSTATION and FILESERVER

As the TSM Backup/Archive client on workstation Cairo (continuous remote data protection) and the TSM Backup/Archive client scheduler service on file server Izmir (“TSM-only” data protection) have *different tasks to perform*, the TSM client nodes CAIRO_WS and IZMIR_FS should belong to *different TSM policy domains*. This ensures that the files being backed up by TSM node CAIRO_WS and TSM node IZMIR_FS respectively have distinct version settings and retention periods regarding their initial source of data.

Table 4-2 on page 161 shows the different parameter settings of copy group STANDARD in policy domains WORKSTATIONS and FILESERVER. For more information about defining policy domains, policy sets, management classes, and copy groups, please refer to Chapter 5, “Administrative Commands”, in *IBM Tivoli Storage Manager for Windows Administrator’s Reference*, GC32-0783.

Table 4-2 Settings of copy group STANDARD in policy domains WORKSTATION and FILESERVER

Parameter	Copy group settings	
Policy Domain Name	WORKSTATION	FILESERVER
Policy Set Name	WORKSTATION_POL	FILESERVER_POL
Mgmt Class Name	WORKSTATION_MC	FILESERVER_MC
Copy Group Name	STANDARD	STANDARD
Copy Group Type	Backup	Backup
VERExists (Versions Data Exists)	NOLimit	7
VERDeleted (Versions Data Deleted)	NOLimit	2
RETExtra (Retain Extra Versions)	7	30
RETOnly (Retain Only Version)	15	90
MODE (Copy Mode)	Modified	Modified
SERialization (Copy Serialization)	Shared Static	Shared Static
DESTination (Copy Destination)	BACKUPPOOL	BACKUPPOOL

Important:

- Policy domain WORKSTATION:

  The TSM Backup/Archive client on workstation Cairo is used by Tivoli Continuous Data Protection for Files for continuous remote data protection. It back ups the most important files, if they have changed, to TSM server Florence every 60 minutes (see Figure 4-11 on page 144).

  As it cannot be estimated how often a file will really be backed up a day (never, once, or multiple times), a version-based retention of files on TSM server Florence is not suitable. In this case, a time-based retention is more applicable.

  Therefore, copy group parameters VERExists and VERDeleted have been set to NOLimit so that all backup versions of files are retained on TSM server Florence until the time-based retention periods, defined by copy group parameters RETExtra 7 and RETOnly 15, are exceeded.

- Policy domain FILESERVER:

  The TSM Backup/Archive client scheduler on file server Izmir runs once a night throughout the week (see "Define TSM client schedule for node IZMIR_FS" on page 168). For this reason, a version-based instead of a time-based file retention is appropriate.

  Making allowance for this fact, the number of backup versions to retain has been limited by specifying copy group parameters VERExists 7 and VERDeleted 2. On the other hand, time-based copy group parameters RETExtra 30 and RETOnly 90 have been set to keep the (inactive) backup versions for these defined periods of time.

Defining policy domains, policy sets, management classes, and copy groups, can be done either via the Integrated Solutions Console (ISC) or by using the TSM administrative command-line client. To use the TSM administrative command-line client for this definitions, please follow these steps:

1. Select **Start** → **Run**, type **cmd**, and click **OK**. A Windows command-line window appears.
2. Change to the installation directory of the TSM Backup/Archive client by entering **cd "\program files\tivoli\tsm\baclient"**.
3. Start the TSM administrative command-line client by entering **dsmadmc**.

Attention: The TSM administrative command-line client (dsmadmc.exe) is not installed by default. If this is the case, refer to Chapter 1, “Installing Tivoli Storage Manager”, in *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788 for details on how to add this component if it was not initially installed.

4. When prompted, enter your administrative user identification (ID) name and password.
5. To define policy domains WORKSTATION and FILESERVER, enter:
   a. **define domain workstation desc='Domain for workstations'**
   b. **define domain fileserver desc='Domain for file server'**
6. To define policy sets WORKSTATION_POL and FILESERVER_POL, enter:
   a. **define policyset workstation workstation_pol desc='Policyset for workstations'**
   b. **define policyset fileserver fileserver_pol desc='Policyset for file server'**
7. To define management classes WORKSTATION_MC and FILESERVER_MC, enter:
   a. **define mgmtclass workstation workstation_pol workstation_mc desc='MC for workstations'**
   b. **define mgmtclass fileserver fileserver_pol fileserver_mc desc='MC for file server'**
8. To define backup copy group STANDARD, enter:
   a. **define copygroup workstation workstation_pol workstation_mc type=backup destination=backuppool verexists=nolimit verdeleted=nolimit retextra=7 retonly=15 serialization=shrstatic**
   b. **define copygroup fileserver fileserver_pol fileserver_mc type=backup destination=backuppool verexists=7 verdeleted=2 retextra=30 retonly=90 serialization=shrstatic**
9. To define archive copy group STANDARD, enter:
   a. **define copygroup workstation workstation_pol workstation_mc type=archive destination=archivepool**
   b. **define copygroup fileserver fileserver_pol fileserver_mc type=archive destination=archivepool**

10. To assign WORKSTATION_MC and FILESERVER_MC as the default management classes, enter:
    a. **assign defmgmtclass workstation workstation_pol workstation_mc**
    b. **assign defmgmtclass fileserver fileserver_pol fileserver_mc**
11. To validate policy sets WORKSTATION_POL and FILESERVER_POL, enter:
    a. validate policyset workstation workstation_pol
    b. **validate policyset fileserver fileserver_pol**
12. To activate policy sets WORKSTATION_POL and FILESERVER_POL, enter:
    a. **activate policyset workstation workstation_pol**
    b. **activate policyset fileserver fileserver_pol**

    and enter **Y** (Yes) for final activation when asked if you wish to proceed.
13. To display information about the active copy group settings, enter:
    a. **query copygroup workstation active workstation_mc f=d**
    b. **query copygroup fileserver active fileserver_mc f=d**

Example 4-6 displays all steps to define policy domains WORKSTATION and FILESERVER as well as their policy sets, management classes, and copy groups.

Example 4-6 Defining policy domains WORKSTATION and FILESERVER

```
IBM Tivoli Storage Manager
Command Line Administrative Interface - Version 5, Release 3, Level 2.0
(c) Copyright by IBM Corporation and other(s) 1990, 2005. All Rights Reserved.

Enter your user id:  admin

Enter your password:  *****

Session established with server FLORENCE: Windows
  Server Version 5, Release 3, Level 2.0
  Server date/time: 04/07/2006 15:34:17  Last access: 04/07/2006 15:30:55


tsm: FLORENCE>define domain workstation desc='Domain for workstations'
ANR1500I Policy domain WORKSTATION defined.

tsm: FLORENCE>define policyset workstation workstation_pol desc='Policyset for workstations'
ANR1510I Policy set WORKSTATION_POL defined in policy domain WORKSTATION.

tsm: FLORENCE>define mgmtclass workstation workstation_pol workstation_mc desc='MC for
workstations'
```

```
ANR1520I Management class WORKSTATION_MC defined in policy domain WORKSTATION, set
WORKSTATION_POL.

tsm: FLORENCE>define copygroup workstation workstation_pol workstation_mc type=backup
destination=backuppool verexists=nolimit verdeleted=nolimit retextra=7 retonly=15
serialization=shrstatic
ANR1530I Backup copy group STANDARD defined in policy domain WORKSTATION, set WORKSTATION_POL,
management class WORKSTATION_MC.

tsm: FLORENCE>define copygroup workstation workstation_pol workstation_mc type=archive
destination=archivepool
ANR1535I Archive copy group STANDARD defined in policy domain WORKSTATION, set WORKSTATION_POL,
management class WORKSTATION_MC.

tsm: FLORENCE>assign defmgmtclass workstation workstation_pol workstation_mc
ANR1538I Default management class set to WORKSTATION_MC for policy domain WORKSTATION, set
WORKSTATION_POL.

tsm: FLORENCE>validate policyset workstation workstation_pol
ANR1515I Policy set WORKSTATION_POL validated in domain WORKSTATION (ready for activation).

tsm: FLORENCE>activate policyset workstation workstation_pol

Do you wish to proceed? (Yes (Y)/No (N)) Y
ANR1514I Policy set WORKSTATION_POL activated in policy domain WORKSTATION.

tsm: FLORENCE>query copygroup workstation active workstation_mc f=d

                Policy Domain Name: WORKSTATION
                   Policy Set Name: ACTIVE
                   Mgmt Class Name: WORKSTATION_MC
                   Copy Group Name: STANDARD
                   Copy Group Type: Backup
             Versions Data Exists: No Limit
            Versions Data Deleted: No Limit
            Retain Extra Versions: 7
              Retain Only Version: 15
                        Copy Mode: Modified
              Copy Serialization: Shared Static
                  Copy Frequency: 0
                Copy Destination: BACKUPPOOL
Table of Contents (TOC) Destination:
     Last Update by (administrator): ADMIN
              Last Update Date/Time: 04/07/2006 17:17:47
                   Managing profile:
                    Changes Pending: No


tsm: FLORENCE>define domain fileserver desc='Domain for file server'
```

```
ANR1500I Policy domain FILESERVER defined.

tsm: FLORENCE>define policyset fileserver fileserver_pol desc='Policyset for file server'
ANR1510I Policy set FILESERVER_POL defined in policy domain FILESERVER.

tsm: FLORENCE>define mgmtclass fileserver fileserver_pol fileserver_mc desc='MC for file
server'
ANR1520I Management class FILESERVER_MC defined in policy domain FILESERVER, set
FILESERVER_POL.

tsm: FLORENCE>define copygroup fileserver fileserver_pol fileserver_mc type=backup
destination=backuppool verexists=7 verdeleted=2 retextra=30 retonly=90 serialization=shrstatic
ANR1530I Backup copy group STANDARD defined in policy domain FILESERVER, set FILESERVER_POL,
management class FILESERVER_MC.

tsm: FLORENCE>define copygroup fileserver fileserver_pol fileserver_mc type=archive
destination=archivepool
ANR1535I Archive copy group STANDARD defined in policy domain FILESERVER, set FILESERVER_POL,
management class FILESERVER_MC.

tsm: FLORENCE>assign defmgmtclass fileserver fileserver_pol fileserver_mc
ANR1538I Default management class set to FILESERVER_MC for policy domain FILESERVER, set
FILESERVER_POL.

tsm: FLORENCE>validate policyset fileserver fileserver_pol
ANR1515I Policy set FILESERVER_POL validated in domain FILESERVER (ready for activation).

tsm: FLORENCE>activate policyset fileserver fileserver_pol

Do you wish to proceed? (Yes (Y)/No (N)) Y
ANR1514I Policy set FILESERVER_POL activated in policy domain FILESERVER.

tsm: FLORENCE>query copygroup fileserver active fileserver_mc f=d

               Policy Domain Name: FILESERVER
                  Policy Set Name: ACTIVE
                  Mgmt Class Name: FILESERVER_MC
                  Copy Group Name: STANDARD
                  Copy Group Type: Backup
            Versions Data Exists: 7
           Versions Data Deleted: 2
           Retain Extra Versions: 30
             Retain Only Version: 90
                       Copy Mode: Modified
              Copy Serialization: Shared Static
                  Copy Frequency: 0
             Copy Destination: BACKUPPOOL
Table of Contents (TOC) Destination:
     Last Update by (administrator): ADMIN
```

```
            Last Update Date/Time: 04/07/2006 17:32:23
                 Managing profile:
                  Changes Pending: No

tsm: FLORENCE>
```

Register TSM client nodes CAIRO_WS and IZMIR_FS

Before the TSM Backup/Archive clients on workstation Cairo and file server Izmir can connect successfully to TSM server Florence, their TSM client node names CAIRO_WS and IZMIR_FS need to be registered on the TSM server first.

To do so, the TSM administrative command-line client (dsmadmc.exe) can be used again:

1. Enter:
   a. **register node CAIRO_WS CAIRO_WS contact="Admin of Florence" domain=workstation**
   b. **register node IZMIR_FS IZMIR_FS contact="Admin of Florence" domain=fileserver**

   to register TSM node names CAIRO_WS and IZMIR_FS and assign them to policy domains WORKSTATION and FILESERVER, respectively.
2. To display information about the registered TSM node names, enter:
   a. **query node cairo_ws**
   b. **query node izmir_fs**

Example 4-7 shows the steps to register TSM node names CAIRO_WS and IZMIR_FS on TSM server Florence, and some information about those nodes using the **query node** command.

Example 4-7 Registering TSM client nodes CAIRO_WS and IZMIR_FS

```
tsm: FLORENCE>register node CAIRO_WS CAIRO_WS contact="Admin of Florence" domain=workstation
ANR2060I Node CAIRO_WS registered in policy domain WORKSTATION.
ANR2099I Administrative userid CAIRO_WS defined for OWNER access to node CAIRO_WS.

tsm: FLORENCE>register node IZMIR_FS IZMIR_FS contact="Admin of Florence" domain=fileserver
ANR2060I Node IZMIR_FS registered in policy domain FILESERVER.
ANR2099I Administrative userid IZMIR_FS defined for OWNER access to node IZMIR_FS.

tsm: FLORENCE>query node cairo_ws

Node Name              Platform     Policy Domain      Days Since     Days Since     Locked?
                                    Name               Last Acce-       Password
                                                            ss            Set
-------------------    --------     --------------     ----------     ----------     -------
CAIRO_WS               (?)          WORKSTATION              <1             <1       No

tsm: FLORENCE>query node izmir_fs

Node Name              Platform     Policy Domain      Days Since     Days Since     Locked?
                                    Name               Last Acce-       Password
                                                            ss            Set
-------------------    --------     --------------     ----------     ----------     -------
IZMIR_FS               (?)          FILESERVER               <1             <1       No

tsm: FLORENCE>
```

Define TSM client schedule for node IZMIR_FS

After the TSM scheduler service and TSM Backup/Archive Client Acceptor Daemon (CAD) have been successfully installed on file server Izmir (see “File server (Izmir)” on page 150), a TSM client schedule needs to be defined on TSM server Florence. This schedule runs on a daily basis, making an incremental backup of file server Izmir (TSM node name IZMIR_FS), and sending the files residing on shared network drive E: to TSM server Florence for long-time data retention.

In Table 4-3 on page 169, you can see the used parameters and their values for the definition of TSM client schedule FS_DAILY_INCR.

Table 4-3 Settings of TSM client schedule FS_DAILY_INCR

Parameter	Value
Policy Domain Name	FILESERVER
Schedule Name	FS_DAILY_INCR
Description	Daily incr. schedule of file server Izmir
Type	Client
Action	Incremental
Start Date/Time	22:00:00
Duration/Units	5 Hour(s)
Period/Units	1 Day(s)
Day of Week	Any

Follow these steps to define TSM client schedule FS_DAILY_INCR and to associate TSM node name IZMIR_FS with it using the TSM administrative command-line client (dsmadmc.exe):

1. Enter **`define schedule fileserver fs_daily_incr type=client desc='Daily incr. schedule of file server Izmir' action=incremental starttime=22:00 duration=5 durunits=hours period=1 perunits=days dayofweek=any`** to define TSM client schedule FS_DAILY_INCR.
2. To associate TSM node name IZMIR_FS with TSM client schedule FS_DAILY_INCR, enter **`define association fileserver fs_daily_incr izmir_fs`**.
3. Enter **`query schedule fileserver fs_daily_incr`** for querying information about TSM client schedule FS_DAILY_INCR.
4. To see the TSM node name(s) associated with TSM client schedule FS_DAILY_INCR, enter **`query association fileserver fs_daily_incr`**.

Steps 1 through 4 are displayed in Example 4-8.

Example 4-8 Defining daily TSM client schedule FS_DAILY_INCR for TSM node name IZMIR_FS

```
tsm: FLORENCE>define schedule fileserver fs_daily_incr type=client desc='Daily incr. schedule
of file server Izmir' action=incremental starttime=22:00 duration=5 durunits=hours period=1
perunits=days dayofweek=any
ANR2500I Schedule FS_DAILY_INCR defined in policy domain FILESERVER.

tsm: FLORENCE>define association fileserver fs_daily_incr izmir_fs
ANR2510I Node IZMIR_FS associated with schedule FS_DAILY_INCR in policy domain FILESERVER.

tsm: FLORENCE>query schedule fileserver fs_daily_incr

Domain         *   Schedule Name      Action   Start Date/Time        Duration   Period   Day
------------   -   ----------------   ------   -------------------   --------   ------   ---
FILESERVER         FS_DAILY_INCR      Inc Bk   04/07/2006 22:00:00       5 H      1 D    Any

tsm: FLORENCE>query association fileserver fs_daily_incr

Policy Domain Name: FILESERVER
     Schedule Name: FS_DAILY_INCR
  Associated Nodes: IZMIR_FS


tsm: FLORENCE>
```

Last steps

After all definitions have been made, the TSM Backup/Archive client on workstation Cairo and the TSM scheduler on file server Izmir can contact TSM server Florence for storing their data. There are many ways to check if everything is working fine by using the TSM administrative command-line client (dsmadmc.exe). Among them are querying the TSM server for the status of scheduled and completed events, and to check if the file spaces have been created:

1. Enter **`query event fileserver fs_daily_incr`** to display events for TSM client schedule FS_DAILY_INCR.
2. To display information about the file spaces on TSM server Florence, enter **`query filespace`**.

Example 4-9 shows the output of commands **query event** and **query filespace**.

Example 4-9 Querying TSM server Florence for scheduled events and file spaces

```
tsm: FLORENCE>query event fileserver fs_daily_incr

Scheduled Start          Actual Start             Schedule Name     Node Name         Status
-------------------      -------------------      -------------     -------------     ---------
04/07/2006 22:00:00      04/07/2006 22:01:01      FS_DAILY_INCR     IZMIR_FS          Completed

tsm: FLORENCE>query filespace

Node Name        Filespace      FSID    Platform    Filespace    Is Files-     Capacity      Pct
                 Name                               Type           pace          (MB)      Util
                                                                 Unicode?
-------------    -----------    ----    --------    ---------    ---------    --------    -----
CAIRO_WS         \\cairo\c$        1    WinNT       NTFS           Yes         4,996.7     90.1
CAIRO_WS         \\cairo\d$        2    WinNT       NTFS           Yes        29,706.1     14.3
IZMIR_FS         \\izmir\e$        1    WinNT       NTFS           Yes       997,888.      3.3
                                                                                    2

tsm: FLORENCE>
```

The output of the **query event** command for TSM client schedule FS_DAILY_INCR displays the status of the event as `Completed`, indicating that the schedule has run successfully.

The **query filespace** output shows that two file spaces (\\cairo\c$ and \\cairo\d$) have been created for TSM node name CAIRO_WS from workstation Cairo and one file space (\\izmir\e$) for TSM node name IZMIR_FS from file server Izmir. As the operating system on both Cairo and Izmir is Windows 2003 using NTFS formatted drives, the platform of the client nodes are displayed as WinNT and the file space types as NTFS.

4.4.3 Summary

By using fictitious company XYZ, Inc. as an example, we have shown a potential scenario of how Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager (TSM) can work either as stand-alone products or hand in hand together:

- On mobile computers or desktop systems, where traditional client-server backup applications are inappropriate, Tivoli Continuous Data Protection for Files is an effective and efficient data protection solution.

- If both programs are installed on the same system, Tivoli Continuous Data Protection for Files can use the TSM Backup/Archive client for continuous remote or scheduled file protection by sending files directly to a TSM server for long-time data retention.
- In case Tivoli Continuous Data Protection for Files and IBM Tivoli Storage Manager operate on different systems, both applications can be used as an excellent complement to each other to get the most benefit out of both products.

Overall, Tivoli Continuous Data Protection for Files is a rather small and easy to configure, but yet very powerful and reliable data protection solution for everyone: private users at home, small and medium businesses, as well as large enterprise companies.

5

Frequently asked questions

This chapter provides answers to questions that are frequently asked by people who use Tivoli Continuous Data Protection for Files as well as people who are considering purchasing the software. There are several sections organized by the following topics:

- Include, exclude, and file lists
- Replication features
- File versions
- IBM Tivoli Storage Manager (TSM)
- Network operations
- Removable disks
- Miscellaneous

Hopefully you will find the answers to all of your questions.

5.1 Include, exclude, and file lists

Here we answer questions regarding include, exclude, and file lists.

Which has higher precedence, include or exclude?

Excludes are processed first. For example, if your include list contains \My Documents\ and your exclude list includes *.jpg, none of your .jpg files will be replicated, even if they are under the \My Documents\ tree.

How can I “include” a certain tree but “exclude” some file types from that tree?

You cannot exclude file types exclusively within a particular tree. If you exclude a file type, it will be excluded from replication no matter what tree it falls under. More complex include/exclude capabilities are under consideration for future versions of the software.

Why is there a file list for both the “Continuous” and the “Scheduled” windows?

Most people want different protection for different types of files. While you could protect all of your changing files with continuous protection, it is probably more sensible to only protect the most important files continuously (files that you change and save directly). We recommend that your continuous file protection file list be a sub-set of the scheduled protection.

Should my Scheduled protection file list also include the same files as my continuous?

Yes, in most cases. Even if you have elected to have “remote protection” on your continuous window, you will probably want to re-capture those files on the scheduled screen as the scheduled protection will make versioned instances on the remote (and the continuous feature will not). This will provide the highest level of protection for your files.

5.2 Replication features

Here we answer questions regarding replication features.

It is not backing up file xyz.xyz; what could be wrong?

99% of the time, this is caused because the exclusion list is excluding more than you expect. Remember, Excludes are processed before Includes. Please check the exclusion list closely, especially the directory path listings. For example, if you exclude \Temp, this will exclude a file named \TemptIsle.doc and all files under the directory path \templates. You should also check the status page for any errors.

How do I know which files have been backed-up?

The Status window shows you the most recent 50 or so transactions. You can also go down through the restore interface, or navigate to the \RealTimeBackup\ folder on your local or network drive using Windows Explorer.

Where are my files stored?

Your files are stored in a directory structure that mirrors their original location. There is a sub-directory named \RealTimeBackup\ created on one of your local disks (if you have selected local protection) and similarly on the remote file server. You can navigate through those trees using Explorer or other tools. Files are stored in their original format but have a unique identifier added to their names so that several versions can be stored simultaneously. You can copy or move those files if you do not want to use the built-in Restore capability. If you do so, we recommend that you change the file name back to a normal style.

Does Tivoli Continuous Data Protection for Files do sub-file (delta) copying?

Yes, you have to enable this feature on the Advanced Settings page. Two different sub-file techniques are available. For Office-type of documents, you *must* also enable “local” protection, since the software needs a prior instance available to do the comparison. For database-like applications (such as e-mail), you need to put the file-extension in the “bitmap” list on that same settings page.

Is the data encrypted in-flight or on-target?

TPC for Files does not currently encrypt data. This feature is scheduled to be available in the 2.2 release. However, if you use the native Windows encryption for your files, Tivoli Continuous Data Protection for Files will back them up like any other files.

Is my data put into some sort of proprietary format so that I need a tool to decompose or recover it?

No. Your data is stored as ordinary files exactly like the originals. You can navigate to the folders yourself to restore a file or use the interface provided.

Does this software add a lot of overhead to my system?

No. Overhead only occurs when files are “saved” and statistically that is a very small percent of the overall operation of your system. Plus, overhead (for continuous protection) is simply an additional “file copy,” tantamount to you hitting Control-S twice in a row in your application. Occasionally, the software may require a bit more processing time, for example, during a Synchronize activity or if you are copying a large number of files to a source location, but these are rare circumstances.

5.3 File versions

Here we answer questions regarding file versions.

How many versions will it store?

On the local system, the default is 20, and this number can be changed/increased by a special command (see *Tivoli Continuous Data Protection for Files Version 2.1. Installation and User's Guide*, GC32-1783). On remote Continuous and Scheduled, you can configure the number from 1-99 on the Advanced Settings page.

Why do my backed-up files have strange names?

In the local save pool area, Tivoli Continuous Data Protection for Files adds a unique tail to each file it copies so that several files with the same base name can be stored (for separate versions). Those strange numbers are a sort of time stamp and thus, when sorted, are in creation-order. When you use the built-in restore capability, Tivoli Continuous Data Protection for Files automatically removes the special part of the name.

Can I do some hand-pruning of the local version pool?

We do not recommend that you do this, but it can be done. Tivoli Continuous Data Protection for Files will immediately realize that the files have been removed and will appropriately account for this with its metric that monitors the pool size.

Can I hand-prune the remote version pool?

Yes, but Tivoli Continuous Data Protection for Files will not realize that those files have been removed until it attempts to delete them itself. Thus, their contribution to the current pool size will be unchanged until we attempt to delete them and thus could cause a pool-purge event sooner than expected.

5.4 IBM Tivoli Storage Manager (TSM)

Here we answer questions regarding IBM Tivoli Storage Manager.

How do I use the IBM Tivoli Storage Manager feature?

IBM Tivoli Storage Manager is the IBM Tivoli Enterprise™ class backup product. If your system already has the IBM Tivoli Storage Manager client code loaded, Tivoli Continuous Data Protection for Files can exploit the IBM Tivoli Storage Manager agent and send changed files directly to a remote IBM Tivoli Storage Manager server for even higher protection. Navigate to the Continuous or Scheduled Configuration windows in the software to enable this feature.

Do I have to have both products installed?

Yes, for the current version of the software, you need to have both Tivoli Continuous Data Protection for Files and the IBM Tivoli Storage Manager client installed on the system you want to protect. This may change in future versions.

Is it recommended to use IBM Tivoli Storage Manager with Tivoli Continuous Data Protection for Files?

It depends. In the current form, it is best to use IBM Tivoli Storage Manager to back up the target file server that captures the data from many Tivoli Continuous Data Protection for Files workstations. Using both together on a workstation is probably too heavy-handed and might adversely affect the IBM Tivoli Storage Manager versioning policy. Using both on a file server seems sensible. In a future Tivoli Continuous Data Protection for Files version that has IBM Tivoli Storage Manager support directly built in, it could be the preferred solution for high volume ISP situations.

How do I restore from IBM Tivoli Storage Manager?

If you have IBM Tivoli Storage Manager installed and have activated Tivoli Continuous Data Protection for Files to push data into IBM Tivoli Storage Manager, you can retrieve that data using the normal IBM Tivoli Storage Manager client GUI. Currently, Tivoli Continuous Data Protection for Files does not provide an interface for restoring from IBM Tivoli Storage Manager, but that feature is anticipated to be in a future version.

I have IBM Tivoli Storage Manager loaded but Tivoli Continuous Data Protection for Files does not seem to be backing up files - they are just pending

Ensure your client node has the option passwordaccess set to generate.

I cannot select the IBM Tivoli Storage Manager option box

You probably do not have the IBM Tivoli Storage Manager client installed on your workstation. It must be installed in order for the option to be enabled.

It says IBM Tivoli Storage Manager is running, but I do not see anything happening

It could be that IBM Tivoli Storage Manager is stuck or trying to prompt. If this is the case, you may need to kill dsmc.exe from the task manager. It could also be making progress and it just has many files to move. The interface does not currently show process or status, such as which file it is currently processing. However, there are some log files that accumulate in the install directory as IBM Tivoli Storage Manager runs that might yield a clue. Look for * TSM * files in your install directory.

5.5 Network operations

Here we answer questions regarding network operations.

If I change my remote target while not in the network and there are already files pending to the old one, what happens?

The system remembers the old target and will keep trying. This could clog up your system if the old target is forever unavailable and you probably should go to the Advanced Activity page and abort the queue.

What happens if I am not always connected to a network?

Tivoli Continuous Data Protection for Files will queue up the list of files that need to be moved to either the remote file server or the IBM Tivoli Storage Manager server. Once you are reconnected, it will automatically send the most current version of the file(s) to the save area.

Can I automate network authentication to avoid problems when I reboot or re-login?

Yes. See your Windows User's guide or your network administrator for information about managing passwords and network connections automatically.

I have changed network targets a few times, and I think the system is confused. How can I get it to forget about bad targets?

Go to the Advanced Activity page and click the **Abort** button.

Why does it say NetWait?

Because Tivoli Continuous Data Protection for Files is getting some sort of network error. From a command line, try to access the current target area yourself. It may be that you have not authenticated correctly or that you were using a drive letter when you saved your configuration and now that drive letter is invalid.

5.6 Removable disks

Here we answer questions regarding removal disks.

Can I use a removable disk instead of a network target?

Yes. Be sure to have it hooked up and available when you do your configuration and click the **Save and Next** button, or you can visit the Configuration window later and click the **Save and Next** button again. At save time, we plant a signature on the disk so that we will not mistakenly send data into another removable device (such as your digital camera) when it is plugged in instead.

I am using a removable drive as my remote target and it is stuck in NetWait

It is possible that your drive was not saved properly in the initial configuration. You can check your removable drive to see if a \RealTimeBackup\ folder was created there. If not, go to the Configuration window in Tivoli Continuous Data Protection for Files and re-save in order to re-create a \RealTimeBackup\ folder on the target.

5.7 Miscellaneous

Here we answer questions about miscellaneous items.

I really want to stop Tivoli Continuous Data Protection for Files from operating for a while, but I do not want to uninstall it

There is now a pause feature; right-click the systray icon and select pause/resume as needed. Or, you can kill filepathsrv from the Windows task manager; no accumulation or monitoring will take place. Then simply log out of your current Windows session and log back in to have the monitoring start again.

I want to see more history than the status screen shows

Examine the file replication.log file in the installation directory for the last 1.3 MBs of transactions.

If I save a large document 20 times while on an airplane, will it attempt to move 20 copies to my remote target when I reconnect?

No, only the most recent copy will move to the network.

What is this thing called FilePath?

The underlying technology of Tivoli Continuous Data Protection for Files is called FilePath. FilePath is real-time file system filter driver that wraps around any file system on any platform and extends the basic features of that file system.

What is “fp”?

“fp” is shorthand for FilePath. Some internal components are called “fp” and use “fp” as a prefix.

What about protecting databases and business applications?

We have tested and qualified client-side e-mail applications such as Outlook® and Notes. Tivoli Continuous Data Protection for Files will move only the changed blocks at either application-close time or at the scheduled interval. The “bitmap” list on the advanced page can be increased to capture other file types such as databases, although formal testing has not been done as of the 2.1.3.0 software. CDP does not quiesce databases or do anything special, but it will eventually get 100% of the changed blocks to the target (no data is ever lost, even if the application is heavily in-use when the backup occurs). CDP does not version the database at the target and so a user will probably want to run a snapshot there or back that up via a traditional mechanism. Why then even use CDP for databases? Because it is the highest-performance, least-impact method to essentially replicate a large file/database to another target (thereby providing protection in the event of the loss of the primary copy).

Will this work with Tivoli SANergy or similar software for LAN-free backup?

Yes. What is Tivoli SANergy? Tivoli SANergy allows LAN network connections to move the data payload over an overlaid SAN fabric if present, thus achieving very high data transfer rates.

I want to install a new version; do I have to uninstall?

No. You can install over an existing installation. All of your data and configuration will be preserved.

If I uninstall will all of my data be removed?

No. It is all left where it was.

I get “page not found” in my browser when I open the GUI

One possible cause is that “localhost” is not resolving correctly. Try `http://127.0.0.1:9003`. If that does not work, check to see if the service is running

My file names are not displayed correctly

Make sure that your browser settings are not overriding some default. All text in Tivoli Continuous Data Protection for Files is presented in UTF-8 and should display correctly.

I worry that there is some interaction problem with the Tivoli Continuous Data Protection for Files driver and some other software (perhaps blue screening)

Move the fp.sys driver to a different name and reboot (perhaps from safe mode).

6

Upcoming features

This chapter describes the features that will be available in Tivoli Continuous Data Protection for Files V2.2, which is due to be released in June 2006. As of the writing of this redbook, the new features include:

- Translation
- Encryption
- Web-based Distributed Authoring and Versioning (WebDAV)
- Improved user interface
- Compression
- Integration with TSM API

Note: The descriptions in this chapter reflect initial design plans. It is possible that some of the features may not be exactly as described here by the time the product is released.

6.1 Translation

Tivoli Continuous Data Protection for Files will be translated into 13 languages, nine Group One languages:

- German
- Spanish
- French
- Italian
- Japanese
- Korean
- Brazilian Portuguese
- Simplified Chinese
- Traditional Chinese

And four Group Two languages:

- Russian
- Polish
- Hungarian
- Czech

The current version of the product is fully globalized, which means that it will operate correctly on foreign operating systems. However, the user interface and all messages are presented in English. Starting in the next version, both the user interface and the messages (including messages sent to the system and event logs) will be translated.

All languages will be installed during the initial product installation, so it will be possible to view the translated version of the product during the initial configuration. It will also be possible to change the language being displayed in the user interface after the product has been installed by changing the default language selected in the browser.

The user interface will display the language selected as default by the browser that is displaying the user interface. The system event messages will be displayed in the language of the operating system. Messages presented in the pop-up area from the system tray icon will be displayed in the language selected for the system's locale. Generally, these will all be the same, but a user can elect to change the language of the browser to something different from the language of the operating system. This way, the language can be changed on-the-fly.

6.2 Encryption

Currently, Tivoli Continuous Data Protection for Files can back up files that have been encrypted by either the operating system or some other program. However, it does not perform any encryption on the files it is backing up. For the new release, Tivoli Continuous Data Protection for Files will have the capability of encrypting files as it performs its various backup activities.

The new encryption function is designed to give Tivoli Continuous Data Protection for Files the ability to encrypt files that are backed up to a remote storage location. Since users do not always have administrative control over the remote storage location, this feature provides them the ability to protect their data from being viewed by other users outside of their control. For example, with the new Web-DAV feature (see 6.3, "Web-based Distributed Authoring and Versioning (WebDAV)" on page 185), users will have the capability to back up sensitive data to their Internet Service Providers (ISPs). ISPs usually provide storage protected by user name and password, but this may not provide a sufficient level of security. Encryption of the data by Tivoli Continuous Data Protection for Files provides another layer of protection that is under the user's control.

When the user selects to turn on the Encryption feature, a dialog will be presented to create a password for the encrypted files. This password will be required to view or access any files that are backed up by Tivoli Continuous Data Protection for Files. Encryption will not be done on files stored on the local pool and will be compatible with both sub-file backups and changed-block backups.

6.3 Web-based Distributed Authoring and Versioning (WebDAV)

Currently, Tivoli Continuous Data Protection for Files can be configured to back up files to a remote file server. The current architecture is flexible when it comes to its ability to send files to remote file system targets. Any remote file system that can be mounted by the operating system can be used as a remote target. The choices of a remote target for Tivoli Continuous Data Protection for Files are limited to the available types of network file systems that the operating system supports. ISPs and other clients have identified a need to use WebDAV as a remote target for Tivoli Continuous Data Protection for Files backups.

The WebDAV protocol provides functionality to create, change, and move documents on a remote server (typically a Web server). This is useful, among other things, for authoring the documents that a Web server serves, but can also be used for general Web-based file storage, that can be accessed from anywhere. Most modern operating systems provide built-in support for WebDAV, making it as easy to use files on a WebDAV server (almost) as though they were stored in a local directory.[1]

Microsoft has been providing a WebDAV client since the release of Windows XP, but this client does not use SSL to provide security. Instead, Microsoft relies on propriety authentication schemes to ensure that a user's password is safe during login and they use a proprietary encryption method to secure the contents of the files as they are being sent.

The Web-DAV feature in Tivoli Continuous Data Protection for Files will provide this security feature as files are being backed up to the remote target. Users will be able to enter a URL for a WebDAV enabled directory on a Web server in the "Remote Backup Location" field for either Continuous or Scheduled protection.

For example:

- http://targetserver.ibm.com
- https://targetserver.ibm.com
- http://targetserver.ibm.com/userdirectory
- https://targetserver.ibm.com/userdirectory

Users with an ISP who provides them with WebDAV accessible Internet storage will be able to use this to feature to back up their data to the server. Users can also restore this data through the CDP interface.

6.4 Improved user interface

Although the Tivoli Continuous Data Protection for Files user interface is fairly straightforward to use, some users have commented that there are a few areas where it could be improved. Additionally, there is a need to have IBM Tivoli products look somewhat similar to make it easier for users to transfer from one product to another. For these reasons, the user interface will be changed to make it even easier to use (see Figure 6-1 on page 187). Some of the windows will be renamed, and Status window will be re-configured to provide a better view of the overall status of replications at a quick glance. This will make it easier for users to monitor and maintain their local and remote backup pools.

[1] Definition excerpted from http://en.wikipedia.org/wiki/WebDAV.

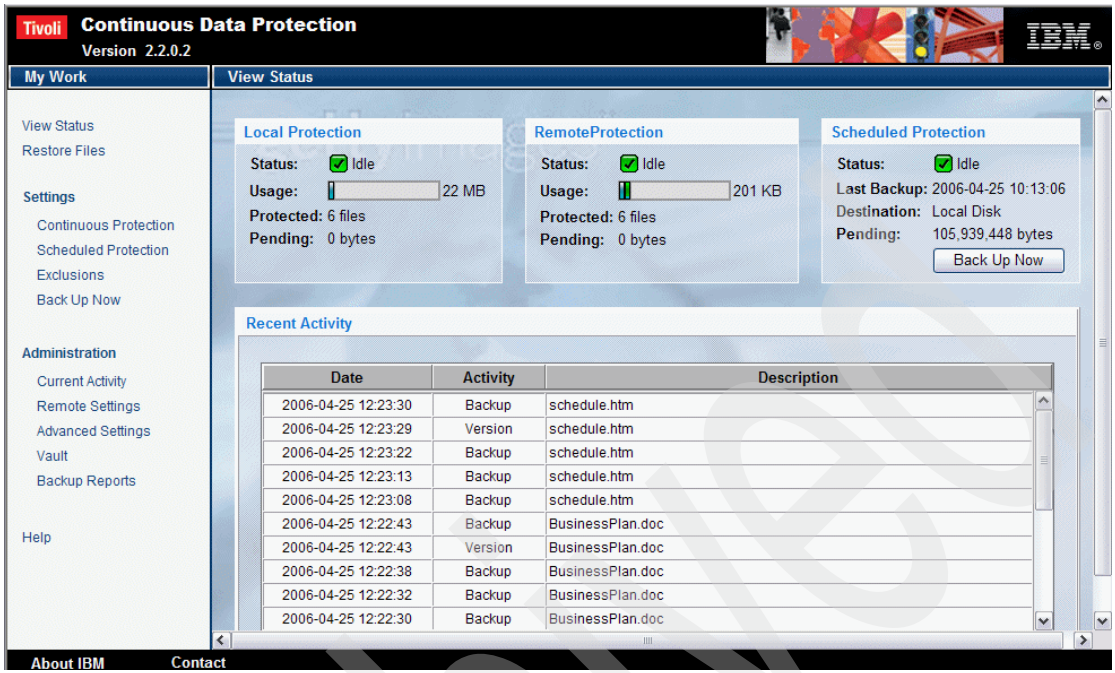


Figure 6-1 Sample window from the new user interface design

6.5 Compression

Currently, Tivoli Continuous Data Protection for Files can back up files that have been compressed by either the operating system or some other program. However, it does not perform any compression on the files it is backing up. For the new release, Tivoli Continuous Data Protection for Files will have the capability of compressing files as it performs its various backup activities.

There will be a check box on the Remote Settings window for the compression setting. Once this box is checked, all files replicated to the remote server, except for bitmap files, will be compressed. This will provide the extra benefit of saving space on the remote server.

Note: You will have to use the Tivoli Continuous Data Protection for Files user interface to restore files that have been compressed on the remote server. This will uncompress the files as they are restored. If you try to copy or move files directly from the remote server, they will be in their compressed form, and unrecognizable to the programs that created them.

6.6 Integration with TSM API

The current version of Tivoli Continuous Data Protection for Files requires that the TSM client be installed on the same machine in order to have Tivoli Continuous Data Protection for Files back up files directly to a TSM server. Starting with Version 2.2, the TSM API will be integrated with Tivoli Continuous Data Protection for Files code so it can communicate directly with a TSM or TSM Express server. This means that the TSM client will no longer be required on the same machine as Tivoli Continuous Data Protection for Files.

Another benefit of this integration is that the restore function within Tivoli Continuous Data Protection for Files can be used to restore files from a TSM server directly. In the current version of the software, users have to use the TSM interface to restore files that Tivoli Continuous Data Protection for Files has backed up into the TSM server. Thus, the new feature will improve both the backup and restore functions by requiring only one product on the local machine, and one interface for both backup and restore.

There are a few other benefits from this integration:

- File transfer progress for individual files will be displayed for TSM backups. Currently, only files backed up to a file server or a USB drive show this level of detail.
- File transfers of individual files can be skipped, using the Skip button on the Tivoli Continuous Data Protection for Files GUI window.
- Settings for throttling and preemption can be applied to files backed up to TSM servers.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

Publications

These publications are relevant as further information sources:

- *IBM Tivoli Storage Manager for Windows Administrator's Reference*, GC32-0783
- *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and Users Guide*, GC32-0788
- *Tivoli Continuous Data Protection for Files Version 2.1. Installation and User's Guide*, GC32-1783

Online resources

These Web sites and URLs are also relevant as further information sources:

- "How To Use NTFS Alternate Data Streams", found at:

  `http://support.microsoft.com/kb/105763/en-us`

- "A Programmer's Perspective on NTFS 2000 Part 1: Stream and Hard Link", found at:

  `http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnfiles/html/ntfs5.asp`

- Sysinternals Web site

  `http://www.sysinternals.com/utilities/debugview.html`

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

A
Accidental file deletion 3
Advanced Settings panel 40
Alternate Data Streams (ADS) 98
Archive retention 12

C
Client Acceptor Daemon (CAD) 134, 152
COMMMethod TCPIP 76
Compression 187
continuous data protection
  default location 27
continuous data protection (CDP) 18, 27, 58, 78, 82
continuous protection 30, 46, 78, 114, 132, 174, 176
Current Activity panel 48

D
data loss 4
data protection 134, 138, 142
default exclusion list 35
deployment 29
dsm.opt 148, 152
dsm.smp file 76
dsmadmc.exe 169
dsmcutil install 156

E
Encryption 185
event log 80
exclusion list 19, 27, 140, 175
external USB 69, 139–140

F
File corruption 3
File FPcommand.bat 113
file server 27–28, 64, 67, 131, 133–134, 175, 177
  shared network drive 134
  UNC naming specification 75
File server issues 72
FilePath agent 115–116
  interactive mode 119
fine tuning 41
firewire 122
firewire port 123
fp.sys 18
fpa.txt 19
fpcommands.xml 130
FPL_META isHit 120
Frequently Asked Questions 173

G
General 2
Graphical User Interface (GUI) 55, 110, 177, 181

H
High-priority files 11
HTML listener 24

I
IBM 131
IBM Tivoli Storage Manager
  client 75, 78–79, 105
  client option 93, 95
  feature 177
  include/exclude list 97
  option box 178
  Pending activities 83
  server 177
IBM Tivoli Storage Manager (TSM) 75, 90, 93–95, 102, 114, 142, 150, 177–178
IBM Tivoli Storage Manager client 177
IBM TotalStorage Open Software Family 8
improved user interface 186
include list 174
inclusion list 19, 26
incremental backup 168
Installation 29
Installation directory 18, 23, 89–90, 94, 101, 149, 154, 180
installation directory
  file replication.log file 180
Integrated Solutions Console (ISC) 162

ISP connection 124

K
kernel layer 19

L
local disk for protection 3
local drives 153
Local pool log file 111
log file 51, 94, 97, 178
loss of productivity 4
LUN (logical unit number) 15

M
Microsoft Developer Network (MSDN) 98

N
NAS (Network Attached Storage) 15
NetWait 179
network authentication 178
network file system 3
Network operations 178
New Technology File System (NTFS) 98
No server component 13
node name 76–77, 135–136
Non-privileged users 54

O
Open architecture 13
option Subdir 93

P
Passwordaccess generate 82
passwordaccess prompt 82
Point-in-time restore 12
Policy domain
  FILESERVER 162, 166
  Workstation 162, 164
Policy domain definitions 160
port conflicts 55

Q
query actlog 105

R
Real-time data protection 12
RealTimeBackup folder 28, 42, 72, 138, 142–143, 147
  first level 42
Redbooks Web site 189
  Contact us xvii
Reduced loss of data 14
remote backup
  activites 50
  destination 151
  location 68, 71, 133–134
  option 27
  target 47, 67–68
remote backup location 147
remote file server 11
remote machine protection 3
remote office servers 7
remote space configuration settings 146
remote space configuration setup 140
remote target 24, 28, 67, 111, 132, 178–179
  default configuration 40
  enough space 34
remote version pool 177
Remote versions 11
Removable disk issues 68
removable storage device 123
replication 1
replication features 175
Replication problems 67
Reports panel 50
Restore panel 43
Restoring files 43

S
SAN (Storage Area Network) 15
schedule 169
schedule protection settings 139
scheduled configuration settings 144
scheduled protection 19, 21, 74, 78, 82, 110–111, 114, 174
  configuration options 34
  IBM Tivoli Storage Manager 113
  summary section 110
scheduled protection file list 174
Scheduled Protection table 47
Status panel 46
synchronize 36

T

TCPPort 1500 76
Tivoli Continuous Data Protection 43, 54, 64, 78
  installation directory 100
Tivoli Continuous Data Protection for Files 2, 177 121
  advanced configuration 38
  benefits 6, 15
  capabilities 18
  Case studies 121
  Comparison with other backup solutions 3
  configuration 30
  Continuous protection 31
  Current Activity panel 48
  default port 56
  Exclusions 35
  how it works 9
  How to run a trace 115
  IBM Tivoli Storage Manager issues 75
  IBM Tivoli Storage Manager working together 131
  installation 29
  installation issues 53
  local disk for protection 3
  main features 12
  Modifying start.html 62
  network file system 3
  overview 2
  port conflicts 55
  Recommended configuration 30
  replication issues 67
  Reports panel 50
  Restore panel 44
  Status panel 46
  Synchronize panel 36
  Trace syntax 116
  tracing 115
  troubleshooting methods 51
  Unique differentiators 15
  use case scenarios 121
    Multiple computers in a home or small business 124
    Multiple users in a large enterprise environment 126
    Single computer with an ISP connection 124
    Single computer with no network connection 122
    single-user environment 122
    with IBM Tivoli Storage Manager 131
  using 43
  value proposition 13
  Version 2.2 183
  what is it? 2
  why is it needed? 4
Tivoli Storage Manager (TSM) 51, 75, 131–132, 177–178
tracing 115
Tracing facilities 115
traditional backup 1
Transient networks 73
Translation 183
TSM Backup/Archive client 75, 77–78, 82, 88, 134, 149, 152–154
  backup session 108
  error 94, 97
  error log 99
  error log file 108
  GUI 90, 92, 155
  GUI executable file 90
  installation 76
  installation directory 89, 105
  log file 94, 103
  node name 136, 168
  node password 136
  option SUbdir 93
  options DOMain 153
  process dsmc.exe 84
  proper communication 91
  scheduler 134, 152
  scheduler service 78, 135, 142, 147, 152
  session 105, 108
TSM Backup/Archive client GUI 90
TSM Backup/Archive command line 100
TSM backups 28
TSM client
  Acceptor Daemon 156
  options 148
  schedule 160, 169
  Service Configuration Utility 155
  Services 156–157
TSM client service 156
  installed 160
TSM interval 28
TSM node name 171
TSM scheduler 170
TSM scheduler service 134, 152
TSM server 25, 27, 75–76, 131, 134, 152

activity log 104–105
connection problems 87
defined schedule 135
name 136
policy definitions 135
registered administrator 104
specific definitions 135
Successful communication 91
TCP/IP address 77
TCP/IP port address 77

U

unforeseen disasters 3
Universal Naming Convention (UNC) 68, 74
Unwanted file alteration 3
Upcoming features 183
USB 122
USB device 123
user id 82, 88, 148–149

V

Vault 38
versioned files 11
Versioning of files 12
virus 16

W

WebDAV (Web-based Distributed Authoring and Versioning) 185
Windows 2000 159
Windows 2003 159
Windows registry 55–56, 59, 149–150
default port 56
necessary changes 60
Windows Taskbar 83
Windows XP 159
workstation 142–144
workstation_pol 164

IBM Redbooks

Deployment Guide Series: Tivoli Continuous Data Protection for Files

(0.2”spine)
0.17”<->0.473”
90<->249 pages

Deployment Guide Series: Tivoli Continuous Data Protection for Files

Redbooks

Step-by-step deployment guide for Tivoli Continuous Data Protection for Files

Discusses best practices for configuration options

User case scenarios, including TSM integration

Tivoli Continuous Data Protection for Files is specifically targeted at end user computers, such as mobile computers and workstations, as well as file servers. It provides continuous data protection of files, providing the highest level of protection possible, yet is simple to use and administer. When files change, Tivoli Continuous Data Protection for Files will make up to three copies of the file (or queue copies to be made later).

This IBM Redbook presents a deployment guide for Tivoli Continuous Data Protection for Files. We cover planning, installing, and troubleshooting of Tivoli Continuous Data Protection for Files for several use case scenarios. In addition, we provide some case studies, including integration with IBM Tivoli Storage Manager, that can be used as a proof of concept or demonstration of the product at a client environment.

The target audience for this redbook is IT Specialists who will be working on Tivoli Continuous Data Protection for Files installations and proof of concepts.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7235-00 ISBN 0738497045